TWO PROBLEMS IN THE THEORY OF CURVES OVER FIELDS OF POSITIVE CHARACTERISTIC

BY

EUIJIN HONG

DISSERTATION

Submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy in Mathematics
in the Graduate College of the
University of Illinois at Urbana-Champaign, 2019

Urbana, Illinois

Doctoral Committee:

Professor Sheldon Katz, Chair
Professor William Haboush, Director of Research
Professor Iwan Duursma, Director of Research
Assistant Professor Christopher Dodd

Abstract

This thesis consists of two parts.

In the first half, we define, so called, generalized Artin-Schreier cover of a scheme X over k. After defining Artin-Schreier group scheme Γ over X, a generalized Artin-Schreier cover is realized as a principal homogeneous space of Γ. We are especially interested in the case when X is $\mathbb{P}^1\backslash\{0, 1, \infty\}$, a thrice punctured plane. An argument of (generalized) Artin-Schreier field extension and its function field arithmetic follows.

The second half is about the coding theory. For a full flag of codes, if it is equivalent to its duals, then it is said to have the isometry-dual property. Introducing characterizations of isometry-dual property for one-point AG codes and its preservation after puncturing at some points, some generalizations in different directions will be given.

To my family

Acknowledgments

Foremost, I would like to express my sincere gratitude to my advisors, Prof. William Haboush and Prof. Iwan Duursma, for their continuous support throughout my Ph.D research. It would not have been possible to finish my thesis without the guidence of my advisors. Prof. Haboush has inspired me in many ways with his immense knowledge and also has helped me broaden my perspective in the research. His encouragement has been the driving force of keeping myself focused on my research. Prof. Iwan Duursma has been a role model for me not only as a teacher but also as a scholar. Having discussions with him has always been intriguing and has given me a great insight.

My thesis was greatly improved with a help of Prof. Maria Bras-Amorós. I truly appreciate her comments and suggestions.

I would like to thank the committee members, Prof. Sheldon Katz and Prof. Christopher Dodd, for their valuable comments on my thesis work. I also thank the departement of Mathematics of the University of Illinois at Urbana-Chamapaign for supporting me financially.

Finally, I would like to express my deep gratitude to my wife and parents who have always been by my side to support me and cheear me up through all the ups and downs of this long journey.

Contents

Part I

Generalized Artin-Schreier Covers

Chapter 1

Preliminaries

Let K be a field of characteristic p. An Artin-Schreier extension F over K is given by a splitting field of an irreducible polynomial of the form $T^p - T - u \in k[T]$ for some $u \in K$. It is a cyclic Galois extension of degree p, whose Galois group is generated by $\sigma(y) = y + \gamma$ where $\gamma \in \mathbb{F}_p$. One feature of the polynomial $T^p - T - u$ is that its nonconstant parts form an additive polynomial whose roots corresponds to elements of the Galois group. We will define a generalized Artin-Schreier extension in this manner, that is, it is a splitting field of a monic irreducible polynomial which is given by a sum of additive polynomial and a constant. For a generalized Artin-Schreier extension, the structure of the roots of its additive parts is highly related to the Galois group of the extension. If the additive parts splits completely in the base field then the root of the additive parts are actually isomorphic to the Galois group of the extension.

In the first section, properties of additive polynomials in general are given. Then in the second section, after briefly reviewing the Artin-Schreier extension, we generalize it. Then we go over theories to compute the genus of a function field. Lastly, we give definition of principal homogeneous space in the theory of schemes which will be used to define generalize Artin-Schreier cover in the next chapter.

1.1 Additive polynomials

This section gives properties of additive polynomials over a Dedekind domain R. For statements and proofs for the case of fields of characteristic p, refer to Chapter 1 of [8].

Let R be a Dedekind domain of characteristic $p > 0$ and K be its field of fraction. Fix an algebraic closure $\overline{K}$ of K. Let $\overline{R}$ be the integral closure of R in $\overline{K}$.

Definition 1.1. A polynomial $f(T) \in R[T]$ is *additive* if $f(a+b) = f(a) + f(b)$ for all $a, b \in \overline{K}$.

The definition of additive polynomial above is sometimes called *absolutely additive*. We use *additive* for short.

The following proposition gives a critical characterization of additive polynomials.

Proposition 1.2 (Proposition 1.1.5 of [8])**.** *If $f(T) \in R[T]$ is additive if and only if it is a linear combination of monomials of the form T^{p^i} for $i \geq 0$.*

Proof. Note that the if part is obvious. Assume that f is additive. Then the polynomial $f(T+a) - f(T) - f(a)$ is identically 0 because it is zero for infinitely many elements in $\overline{K}$. By taking the derivative and evaluating at 0, we get $f'(a) = f'(0)$. So, $f'(a) = c$ is a constant for all $a \in \overline{K}$. Note that $f(0) = 0$ because for a root $\gamma \in \overline{K}$ of $f(T)$, we get $f(\gamma + 0) = f(0) = 0$.

We proceed by induction on degree of f. If $\deg f = 1$, then $f(T) = cT$, so it is of the required form. In general, consider $g(T) := f(T) - cT$, where c is the coefficient of the degree one term of $f(T)$. Then $g'(T) = 0$, so there exists a polynomial $h(T)$ such that $h(T^p) = g(T)$. Considering the injective homomorphism $T \mapsto T^p$, it is clear that $h(T)$ is additive if and only if $h(T^p)$ is also additive. Then $\deg h(T) < \deg f(T)$. Therefore by the induction on the degree of $f(T)$, the polynomial $h(T)$ is linear combination of monomials T^{p^i} and so is $f(T)$. □

The following theorem is called the Fundamental Theorem of Additive Polynomial.

Theorem 1.3 (Theorem 1.2.1 of [8])**.** *Suppose K is infinite. Let $f(T) \in K[T]$ be a sepaable polyonmial with set of roots $\Gamma := \{\gamma_1, \cdots, \gamma_n\} \subseteq \overline{K}$. Then $f(T)$ is additive if and only if Γ is an additive group.*

Proof. Assume that $f(T)$ is an additive polynomial. Then $f(\gamma_i + \gamma_j) = f(\gamma_i) + f(\gamma_j) = 0$. So, the set of roots Γ forms an additive group. Conversely, assume that Γ is a group under addition. Note that $f(T) = \prod_{i=1}^{n}(T - \gamma_i)$. If $\gamma \in \Gamma$, then $f(T + \gamma) = f(T)$. For any arbitaray $y \in \overline{k}$, let

$$g(T) := f(T + y) - f(T) - f(y).$$

Then $\deg g(T) < \deg f(T)$ and $g(T)$ has all Γ as its roots. Then $g(T) = 0$. Since y is arbitrarily chosen from K, it is identically zero. $\square$

Then the following can be obtained.

Corollary 1.4. *Let $f(T) \in R[T]$ be a monic polynomial. Suppose $f(T)$ is separable if it is viewed as a polynomial over K. Then $f(T)$ is additive if and only if the roots $\alpha_1, \cdots, \alpha_n$ of f in $\overline{K}$ forms an additive subgroup in $\overline{R}$.*

Proof. Supoose that $f(T)$ is additive. Then it is also additive as a polynomial over K. From Theorem 1.3 the roots $\{\alpha_1, \cdots, \alpha_n\}$ of $f(T)$ forms an additive group in $\overline{K}$. Then so is in $\overline{R}$. Conversely, if $\{\alpha_1, \cdots, \alpha_n\}$ forms an additive subgroup of $\overline{R}$, it is an additive subgroup of K and $f(T)$ is additive in the sense of $f(T) \in K[T]$. Then it is obviously additive in $R[T]$. $\square$

Definition 1.5. A finite set V of $\overline{R}$ is called an *R-subgroup* if

$$F_V(T) = \prod_{v \in V} (T - v)$$

is a polynomial with coefficients in R.

Example 1.6. For any $n > 1$, the field $\mathbb{F}_{p^n}$ is an $\mathbb{F}_p$-subgroup. It consists of all roots of the polynomial

$$\prod_{v \in \mathbb{F}_{p^q}} (T - v) = T^{p^n} - T \in F_p[T]$$

Proposition 1.7. *Let V and W be additive R-subgroups. Note that they are also finite dimenstional $\mathbb{F}_p$ vector spaces. If $V \cap W = \{0\}$ then $V \oplus W$ is also an additive R-subgroup.*

Proof. Let $v_1, \cdots, v_n$ be an basis of V and $w_1, \cdots, w_m$ be a basis of W over $\mathbb{F}_p$. Then $F_V(T)$ and $F_W(T)$ are given as follow:

$$F_V(T) = \prod_{v \in V} (T - v) = T^{p^n} + a_1 T^{p^n - 1} + \cdots + a_r T^{p^n - r} + \cdots + a_{p^n - 1} T$$

$$F_W(T) = \prod_{w \in W} (T - w) = T^{p^m} + b_1 T^{p^m - 1} + \cdots + b_r T^{p^m - r} + \cdots + b_{p^m - 1} T$$

where all a_i and b_j are in R for $1 \leq i \leq p^n - 1$ and $1 \leq j \leq p^m - 1$. Note that both polynomials have no constant terms because V and W both contain 0. Now we have

$$\begin{aligned} F_{V\oplus W}(T) &= \prod_{\substack{v\in V\\ w\in W}} (T - v - w) = \prod_{v\in V}\prod_{w\in W} \big((T-v)-w\big) \\ &= \prod_{v\in V} F_W(T-v) = \prod_{v\in V} \big(F_W(T) - F_W(v)\big) \end{aligned}$$

The last equality comes from $F_W(T)$ being an additive polynomial.

Let's introduce indeterminates $x_1, \cdots, x_{p^n}$ and $y_1, \cdots, y_{p^m}$ and consider the elementary symmetric functions :

$$\alpha_i(x_1, \cdots, x_{p^n}) = \sum_{1\leq i_1<\cdots<i_l\leq n} \prod_{k=1}^{l} x_{i_k} \text{ for } 1 \leq l \leq p^n$$

$$\beta_j(y_1, \cdots, y_{p^m}) = \sum_{1\leq j_1<\cdots<j_l\leq m} \prod_{k=1}^{l} y_{j_k} \text{ for } 1 \leq l \leq p^m$$

Then

$$\begin{aligned} &\alpha_0(x_1, \cdots, x_{p^n}) = 1 \\ &\alpha_1(x_1, \cdots, x_{p^n}) = \sum_{k=1}^{p^n} x_k \\ &\vdots \\ &\alpha_r(x_1, \cdots, x_{p^n}) = \sum_{1\leq i_1<\cdots<i_r\leq p^n} x_{i_1}x_{i_2}\cdots x_{i_r} \\ &\vdots \\ &\alpha_{p^n}(x_1, \cdots, x_{p^n}) = x_1x_2\cdots x_{p^n} \end{aligned}$$

$$\beta_0(y_1, \cdots, y_{p^m}) = 1$$

$$\beta_1(y_1, \cdots, y_{p^m}) = \sum_{k=1}^{p^m} y_k$$

$$\vdots$$

$$\beta_r(y_1, \cdots, y_{p^m}) = \sum_{1 \le l_1 < \cdots < l_r \le p^m} y_{l_1} y_{l_2} \cdots y_{l_r}$$

$$\vdots$$

$$\beta_{p^m}(y_1, \cdots, y_{p^m}) = y_1 y_2 \cdots y_{p^m}$$

We may write

$$F_X(T) = \prod_{1 \le i \le p^n} (T - x_i) = T^{p^n} + \alpha_1 T^{p^n - 1} + \alpha_2 T^{p^n - 2} + \cdots + \alpha_r T^{p^n - r} + \cdots \alpha_{p^n - 1} T + \alpha_{p^n}$$

$$F_Y(T) = \prod_{1 \le j \le p^n} (T - y_j) = T^{p^m} + \beta_1 T^{p^m - 1} + \beta_2 T^{p^m - 2} + \cdots + \beta_r T^{p^m - r} + \cdots \beta_{p^m - 1} T + \beta_{p^m}$$

Note that $F_X(T) \in R[x_1, \cdots, x_{p^n}, T]^{S^x_{p^n}} = R[\alpha_0, \alpha_1, \cdots, \alpha_{p^n}, T]$ and $F_Y(T) \in R[y_1, \cdots, y_{p^m}, T]^{S^y_{p^m}} = R[\beta_0, \beta_1, \cdots, \beta_{p^m}, T]$, where $S^x_{p^n}$ and $S^y_{p^m}$ act as permutations on x_i's and y_j's respectively.

Consider the function

$$F_{X+Y}(T) = \prod_{\substack{1 \le i \le p^n \\ 1 \le j \le p^m}} (T - x_i - y_j) \in R[\alpha_i, \beta_j, T]$$

Then $F_{X+Y}(T) \in R[x_i, y_j, T]^{S^x_{p^n}} \cap R[x_i, y_j, T]^{S^y_{p^m}} = R[\alpha_i, \beta_j, T]$.

Now, let's evaluate x_i, $1 \le i \le p^n$ by all distinct $v \in V$ and evaluate y_j, $1 \le j \le p^m$ by all distinct $w \in W$ and write the value of α_i and β_j by this evaluation by $\alpha_i(V)$ and $\beta_j(W)$. Then obviously $\alpha_i(V) = a_i$ and $\beta_i(W) = b_i$. Thus by this evaluation, all α_i and β_j are in R. Then

$$F_{V \oplus W}(T) = \prod_{\substack{v \in V \\ w \in W}} (T - v - w) \in R[\alpha_i(V), \beta_j(W), T] = R[a_i, b_j, T] = R[T]$$

Therefore $V \oplus W$ is also an additive R-subgroup. $\square$

Proposition 1.8. *For finite additive R-subgroups V and W, the set $F_W(V) := \{F_W(v) : v \in V\}$ is also an additive R-subgroup.*

Proof. It is obvious that the set $F_W(V)$ forms an additive group. To prove that it is an R-subgroup, we need to show that the coefficients of the following polynomial is in R :

$$\prod_{v \in V}(T - F_W(v))$$

Using the notation of the proof of the previous theorem, we may put the polynomial as the following form

$$\prod_{1 \le i \le p^n}(T - F_Y(x_i))$$

It is enough to show that the coefficients of the polynomial is preserved by the action of $S^x_{p^n}$ and $S^y_{p^m}$ which are permutation groups on x_i's and y_j's respectively. However, the coefficients of the polynomial is given by $\alpha_0(F_W(x_1), \cdots, F_W(x_{p^n})), \cdots, \alpha_{p^n}(F_W(x_1), \cdots, F_W(x_{p^n}))$. For example,

$$\alpha_2(F_W(x_1), \cdots, F_W(x_{p^n})) = \sum_{i<j}\Big(\prod_{y \in Y}(x_i - y)\prod_{y \in Y}(x_j - y)\Big)$$

Since this polynomial is symmetric with respect to x_i's and y_j's separately, it is also in $R[\alpha_i, \beta_j, T]$. Therefore the original polynomial is in $R[a_i, b_j, T] = R[T]$, so it is and R-subgroup. □

Remark 1.9. For additive R-subgroups V and W with $V \cap W = \{0\}$ we have the following relation

$$F_{V \oplus W}(T) = F_{F_W(V)}(F_W(T)) = F_{F_V(W)}(F_V(T))$$

In [11], Ore gives the following theorem.

Theorem 1.10. *For any $g(T) \in K[T]$, there exists an additive polynomial $f(T) \in K[T]$ such that $g(T)|f(T)$.*

1.2 Generalized Artin-Schreier extension

According to the Artin-Schreier theorem, every degree p extension of a field of characteristic p is a splitting field of an irreducible polynomial of the form

$T^p - T - u$ for some u in the base field. In this section we generalize it. Use the following notations throughout this section. Let K/k be a function field, that is, K is an extension with transcendental degree 1 over k.

P, P', Q	Places of the function field K/k
$\mathbb{P}_K$	Set of places of K/k
$d(P'\|P)$	Different exponent of P' over P
$e(P'\|P)$	Ramification index of P' over P
$f(P'\|P)$	Relative degree of P' over P

The following theorem states the Artin-Schreier extension and an explicit formula computing the genus of the function field given by the function field extension.

Theorem 1.11 ([12], Proposition 3.7.8, Artin-Schreier)**.** *Let $u \in K$ such that the polynomial $T^p - T - u \in K[T]$ has no roots in K. Let L be a splitting field of K by the polynomial and $y \in L$ be the root of the polynomial.*

$$m_P := \begin{cases} m, & \text{if there exists } z \in F \text{ such that} \\ & \qquad v_P(u - (z^p - z)) = -m \text{ with } m \not\equiv 0 \bmod p \\ -1, & \text{if there exists } z \in F \text{ such that } v_P(u - (z^p - z)) > 0 \end{cases}$$

Then the following hods:

(a) L/K is a cyclic Galois extension of degree p and the generator of $Gal(L/K)$ is given by

$$\sigma : y \mapsto y + 1$$

(b) P is unramified in L/K if and only if $m_P = -1$.

(c) P is totally ramified in L/K if and only if $m_P > 0$. If $P'|P$, in this case, then

$$d(P'|P) = (p-1)(m_P - 1)$$

(d) If at least one $Q \in \mathbb{P}_K$ satisfies $m_Q > 0$, then K is algebraically closed in L and

$$g' = p \cdot g + \frac{p-1}{2}\Big(-2 + \sum_{P \in \mathbb{P}_F} (m_P + 1) \cdot \deg P \Big)$$

here g and g' are the genus of the function field K/k and L/k respectively.

We define generalized Artin-Schreier extension as follow.

Definition 1.12. Let K be a field of characteristic $p > 0$. Let Γ be an additive K-subgroup. Then by definition $f_\Gamma(T)$ is an additive polynomial. Let $u \in K$ be such that $f(T) - u$ is irreducible over K. The splitting field L of the polynomial $f(T) - u$ over K is called a *generalized Artin-Schreier* extension.

One example of generalized Artin-Schreier extension is an elementary abelian p-extension where Γ is given by $\mathbb{F}_{p^n}$, so the polynomial is of the form

$$f_\Gamma(T) - u := T^{p^n} - T - u \in K[T].$$

Proposition 1.13 (1.1 Proposition of [5])**.** *Let $\mathbb{F}_{p^n} \subseteq K$ and L/K is elementary abelian extension of degree p^n. Then the extension L/K is given by the quotient field of an irreducible polynomial*

$$T^{p^n} - T - u$$

for some $u \in K$.

Proposition 1.14 (1.2 Proposition of [5])**.** *Let L/K be an elementary abelian p-extension given by an irreducible polynomial $T^{p^n} - T - u$. Then there exist total $t = \dfrac{(p^q - 1)}{(p - 1)}$ number of degree p subextensions of L/K. Write them as $E_1, \cdots, E_t$. Moreover, each subextension E_i is given by $E_i = K(\alpha_\mu)$ where for $\mu \in \mathbb{F}_{p^n}^*$,*

$$\alpha_\mu := (\mu\alpha)^{p^{n-1}} + (\mu\alpha)^{p^{n-2}} + \ldots + (\mu\alpha)^p + \mu\alpha$$

where α is a root of $T^{p^n} - T - u = 0$.

The genus of the function field given by the extension of $f_\Gamma(T) - u$ is given explicitly by the following theorem.

Theorem 1.15 ([5], 2.1 Theorem)**.** *Let L/K be an elementary abelian p-extension of degree p^n, i.e. L is a splitting field of the polynomial of the form*

$f(T) - u$ of degree p^n such that k is also the constant field of L. Then

$$g(L) = \sum_{i=1}^{t} g(E_i) - \frac{p}{p-1}(p^{n-1} - 1) \cdot g(L)$$

Definition 1.16. A generalized Artin-Schreier extension L/K given by $f_\Gamma(T) - u$ is called *split* if $\Gamma \subseteq K$.

In the above case, the group Γ is a subset of the field K. In general, if Γ is not in K then the quotient field $K[T]/\langle f_\Gamma(T) - u\rangle$ is not isomorphic to the splitting field of $f_\Gamma(T) - u$.

Remark 1.17. If α is a root of $f_\Gamma(T) - u$, then all other roots are of the form $\alpha + \gamma$ for some $\gamma \in \Gamma$. So, the splitting field of $f_\Gamma(T) - u$ contains both α and Γ regardless of Γ being a subset of K or not.

Proposition 1.18. *Any finite algebraic field extension M of K is a subextension of generalized Artin-Schreier extension.*

Proof. Let $\alpha_1, \alpha_2, \ldots, \alpha_s$ be the genrator of M over K. Consider the irreducible polynomials $g_1(T), g_2(T), \ldots, g_s(T)$ of $\alpha_1, \alpha_2, \ldots, \alpha_s$ respectively. Let $g(T) = \prod_{i=1}^{s} g_i(T)$. Then by Theorem 1.10, there exists an additive polynomial $f(T)$ which is divisible by $g(T)$. If there exists $u \in K$ such that $f(T) - u$ is irreducible then the splitting field of $f(T) - u$ is a generalized Artin-Schreier extension which contains all $\alpha_1, \alpha_2, \ldots, \alpha_s$. The existance of such u can be proved by the following Proposition by choosing a place P which is not a pole of any of coefficient of $f(T)$ and choose u to have a pole at P. □

The following Proposition gives criteria determining irreducibility of a polynomial. One of its case is especially called *Eisenstein Criterion*.

Proposition 1.19 (Proposition 3.1.15 of [12])**.** *For a function field K/k, consider a polynomial*

$$\phi(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_1 T + a_0$$

with $a_i \in K$. Assume that there exists a place $P \in \mathbb{P}_K$ such that one onf the following holds:

1. *$v_P(a_i) \geq v_P(a_0) > 0$ for $i = 1, \ldots, n-1$, and $\gcd(n, v_P(a_0)) = 1$.*

2. $v_P(a_i) \geq 0$ *for* $i = 1, \ldots, n-1$ *and* $v_P(a_0) < 0$ *and* $\gcd(n, v_P(a_0)) = 1$.

Then $\phi(T)$ *is irreducible over* K.

Lastly, we review the Kummer extension, which is a special type of Galois extension of cyclic group, whose order is prime to the characteristic p. This theorem will be used to compute the genus of anisotropic generalized Artin-Schreier extension.

Theorem 1.20 ([12], Proposition 3.7.3)**.** *Let* k *contains a primitive* n*-th root of unity. Let* L/K *be the splitting field of the polynomial* $T^n - u = 0$*, where there is no such* $w \in K$ *satisfying*

$$u = w^d \text{ for } d|n,\ d > 1$$

Then the following holds:

(a) The extension $L = K(y)$ *over* K *is Galois of degree* n *with cyclic Galois group, where* $y^n - u = 0$*. Automorphisms of* L/K *are given by* $\sigma(y) = \zeta y$*, where* ζ *is a primitive* n*-th root of unity.*

(b) For place $P'|P$*, where* $P \in \mathbb{P}_K$ *and* $P' \in \mathbb{P}_L$*, we have*

$$e(P'|P) = \frac{n}{r_P} \text{ and } d(P'|P) = \frac{n}{r_P} - 1,$$

where $r_P = \gcd(n, v_P(u)) > 0$.

(c) Let g *and* g' *denote the genus of* K/k *and* L/k *respectively, then*

$$g' = 1 + n\Big(g - 1 + \frac{1}{2}\sum_{p \in \mathbb{P}_K} \big(1 - \frac{r_P}{n}\big) \deg P\Big)$$

1.3 Branches, places and genus of a curve

In this section, we introduce the notion of branch in the power series $k((t))$ and use it to define place of an algebraic curve. This will lead us to compute the genus of an algebraic curve. We will follow the exposition of Chapter 4 and 5 of [9].

Let k be a perfect field of characteristic $p > 0$ and $k[[t]]$ be the ring of power series over k. The field of fraction of $k[[t]]$ is denoted by $k((t))$. We state some properties of $k[[t]]$ and $k((t))$.

Remark 1.21. The following properties hold for $k[[t]]$ and $k((t))$.

1. The ring $k[[t]]$ is a UFD.
2. An element $f(t) = f_0 + f_1 t + \cdots$ of $k[[t]]$ for $f_i \in k$ is invertible if and only if $f_0 \neq 0$.
3. Every element of $k((t))$ can be expresses as $t^m f(t)$ where $m \in \mathbb{Z}$ and $f(t)$ is invertible in $k[[t]]$.

Definition 1.22. For $f(t) = f_{i_1} t^{i_1} + f_{i_2} t^{i_2} + \cdots$ in $k[[t]]$, where $f_{i_j} \in k$ with $i_1 < i_2 < \cdots$ and $f_{i_1} \neq 0$, the *order* of $f(t)$ is i_1 denoted by $\mathrm{ord}_t f(t)$.

As a convention, we put $\mathrm{ord}_t 0 = \infty$. Note that an element $f(t)$ in $k[[t]]$ is invertible if and only if $\mathrm{ord}_t f(t) = 0$, that is, it has a nonzero constant term.

Proposition 1.23 (Theorem 4.4 of [9])**.** *The following holds.*

1. *Every k-monomorphism of $k[[t]]$ is of the form*

$$\begin{aligned} k[[t] &\longrightarrow k[[t]] \\ t &\longmapsto \tau \end{aligned}$$

   where $ord_t \tau \geq 1$.

2. *Every k-automorphism of $k[[t]]$ is given as a k-monomorphism with $ord_t \tau = 1$.*
3. *Every k-monomorphism of $k((t))$ is given by k-monomorphism of $k[[t]]$ and the converse is also true, that is, every k-monomorphism of $k((t))$ gives a k-monomorphism of $k[[t]]$ by restriction to $k[[t]]$.*

Definition 1.24. A *branch representation* is a point $(x_0(t) : x_1(t) : x_2(t)) \in \mathbb{P}^3_{k((t))} \backslash \mathbb{P}^3_k$. A branch representation is *special* if $\min\{\mathrm{ord}_t x_i(t)\}$ is zero. In this case a point $P = (x_0(0) : x_1(0) : x_2(0))$ is the *center* of the branch representation.

For a special branch representation $(x_0(t), x_1(t), x_2(t))$, let

$$\begin{aligned} x_0(t) &= a + a_1 t + a_2 t^2 + \cdots \\ x_1(t) &= b + b_1 t + b_2 t^2 + \cdots \\ x_2(t) &= c + c_1 t + c_2 t^2 + \cdots \end{aligned}$$

Definition 1.25. The *order of a special branch representation* $(x_0(t), x_1(t), x_2(t))$ is defined as the positive integer

$$\min\{\mathrm{ord}_t(d_0x_0(t) + d_1x_1(t) + d_2x_2(t)) : \text{ for all } (d_0, d_1, d_2) \in \mathbb{P}^3_k \\ \text{with } d_0a + d_1b + d_2c = 0\}$$

Remark 1.26. If one of the coordinate of $(x_0(t) : x_1(t) : x_2(t))$ is invertible, we define branch representation $(x(t), y(t))$ in affine plane over $k((t))$ in the trivial way by dividing by the invertible component and eliminating the component 1. We define special branch representation in affine coordinates and the center of it in the similar manner.

Definition 1.27. Two branch representations in special affine coordinates $(x(t), y(t))$ and $(\xi(t), \eta(t))$ are *equivalent* if there exists a k-automorphism σ of $k[[t]]$ such that

$$x(t) = \sigma(\xi(t)) \text{ and } y(t) = \sigma(\eta(t)).$$

Two branch represntations are *equivalent* if they are equivalent in the form of special affine coordinates.

Definition 1.28. A branch representation in special affine coordinates $(x(t), y(t))$ is *imprimitive* if there exists a branch representation in special affine coordinates $(\xi(t), \eta(t))$ such that

$$x(t) = \sigma(\xi(t)) \text{ and } y(t) = \sigma(\eta(t))$$

for some k-monomorphism σ with $\mathrm{ord}_t\sigma > 1$.

A branch representation is *imprimitive* if it is imprimitive in the form of special affine coordinates. A branch representation which is not imprimitive is called *primitive*.

The following characterizes primitive branch representations.

Theorem 1.29 (Theorem 4.21 of [9])**.** *A branch representation* $(x(t), y(t))$ *in special affine coordinates is primitive if and only if there is an element of order* 1 *in* $k(x(t), y(t))$.

Definition 1.30. A special affine branch represenation is *reducible* if for any of its equivalent branch representation, say $(x(t), y(t))$, there exists a branch

representation $(\xi(t), \eta(t))$ such that

$$x(t) = \xi(t^m) \text{ and } y(t) = \eta(t^m)$$

for an integer $m > 1$.

The following sereies of theorems will be useful to pick a branch representation of a place of an algebraic curve later:

Theorem 1.31 (Theorem 4.26 of [9]). *Let $p = 0$ or $p > 0$ with $p \nmid n$. A branch representation in special affine coordinates*

$$\begin{aligned} x(t) &= a + t^n, \\ y(t) &= b + b_1 t^{n_1} + b_2 t^{n_2} + \cdots, \end{aligned}$$

is reducible if and only if $\gcd(n, n_1, n_2, \ldots) > 1$.

Theorem 1.32 (Theorem 4.27 of [9]). *Let $p = 0$ or $p \nmid n$. Every branch representation of order n has a special affine coordinate form of the type*

$$x(t) = a + t^n, \;\; y(t) = b + \eta(t)$$

where $ord_t \eta(t) \geq n$.

Theorem 1.33 (Theorem 4.28 of [9]). *Let $p = 0$ or $p \nmid n$. A branch representaion of special affine coordinates of order n is imprimitive if and only if it is reducible.*

Definition 1.34. A *branch* is an equivalence class of primitive branch representations. The *center* and *order* are the center and order of any of its primitive branch representation and do not depend on a choice of branch representations.

Let $\mathcal{F}$ be an irreducible projective plane curve over the field k defined by a homogeneous polynomial $F(X_0, X_1, X_2)$.

Definition 1.35. A branch of a plane curve $\mathcal{F}$ is a branch whose representation $(x_0(t), x_1(t), x_2(t))$ satisfies $F(x_0(t), x_1(t), x_2(t)) = 0$ in $k((t))$.

Theorem 1.36 (Theorem 4.31 of [9]). *The center of a branch of a plane curve is a point of the curve.*

Theorem 1.37 (Theorem 4.32 of [9]). *For a simple point P of $\mathcal{F}$, there exists a unique branch of $\mathcal{F}$ whose center is P.*

Definition 1.38. Let $\mathcal{G}$ be a projective plane curve defined by a homogeneous polynomial $G(X_0, X_1, X_2)$ and let γ be a branch centered at a point P. If $(x_0(t), x_1(t), x_2(t))$ is a representation of γ in a special coordinates, then the *intersection multiplicity* is defined by

$$I(P, \mathcal{G} \cap \gamma) = \begin{cases} \mathrm{ord}_t G(x_0(t), x_1(t), x_2(t)) & \text{if } \gamma \notin \mathcal{G} \\ \infty & \text{if } \gamma \in \mathcal{G} \end{cases}$$

Note that $I(P, \mathcal{G} \cap \gamma)$ doesn't depend on the choice of a representation $(x_0(t), x_1(t), x_2(t))$.

The following theorem gives a method of computing intersection multiplicity of two plane curves $\mathcal{G}$ and $\mathcal{F}$.

Theorem 1.39 (Theorem 4.36 of [9]). *1. Let γ be a branch of $\mathcal{F}$ centered at a simple point P of $\mathcal{F}$ and let $\mathcal{G}$ be any curve. Then*

$$I(P, \mathcal{G} \cap \gamma) = I(P, \mathcal{G} \cap \mathcal{F}).$$

2. If P is a singular point of an irreducible curve $\mathcal{F}$ and $\mathcal{G}$ is a plane curve not containing $\mathcal{F}$ as a component, then

$$I(P, \mathcal{G} \cap \mathcal{F}) = \sum_{\gamma} I(P, \mathcal{G} \cap \gamma)$$

where γ runs over all branch of $\mathcal{F}$ centered at P.

3. If P is a m_P-fold singular point of $\mathcal{F}$ then the number of branches of $\mathcal{F}$ centered at P is bounded above by m_P.

Definition 1.40. $P = (\zeta, \eta)$ is called a *point* if ζ and η is in some extension of the field k. A branch representation is a point in this sense. A point is *constant* if both ζ and η are in k, or otherwise, the point is called *variable*.

A point $P = (\zeta, \eta)$ on the curve $\mathcal{F} = \mathbf{v}(F(X, Y))$ is called *generic* if for every $G(X, Y) \in k[X, Y]$ satisfying $G(\zeta, \eta) = 0$, we have $G(a, b) = 0$ for all constant points $Q = (a, b)$ on $\mathcal{F}$. This is equivalent to $G \equiv 0 \pmod{F}$.

Let k be a field of characteristic p and let Σ be a field of transcendental degree 1 over k.

Definition 1.41. A *model* of Σ is given by $P = (x, y)$ such that $\Sigma = k(x, y)$ and by the curve $\mathcal{F}$ having P as a generic point. We write it as $(\mathcal{F}; (x, y))$.

Let $(\mathcal{F}; (x, y))$ be a model of Σ and $\eta(t))$ be a branch representation of $\mathcal{F}$.

Definition 1.42.

1. A k-monomorphism $\sigma : \Sigma \longrightarrow k((t))$ is a *place representation.*
2. A place representation σ is *primitive* if $(\sigma(x), \sigma(y))$ is a primitive branch representation of $\mathcal{F}$.
3. Two place representations σ and σ' are *equivalent* if there is a k-automorphism ρ of $k((t))$ such that $\sigma = \sigma \circ \rho$.
4. A *place* is an equivalence class of primitive place representations.
5. Write $\mathfrak{P}(\Sigma)$ for the set of all places of Σ.

Remark 1.43. There is a one-to-one correspondence between the places of Σ and the branches of any model of Σ in a natural way. Moreover, if $(\mathcal{F}; (x, y))$ and $(\mathcal{F}'; (x', y'))$ are two models of Σ, then for the birational transformation sending $P = (x, y)$ to $P' = (x', y')$ there is one-to-one correspondence between branches of $\mathcal{F}$ and $\mathcal{F}'$ which is coherent with the correspondence of places of Σ, that is, any two corresponding branches of $\mathcal{F}$ and $\mathcal{F}'$ correspond to the same place of Σ.

With this relation, we can convert computations regarding plces of Σ to those in terms of power series.

For an irreducible curve $\mathcal{F} = \mathbf{v}(F(X, Y))$, and a generic point $P = (x, y)$, let $\mathcal{P}$ be a place of $\Sigma = K(x, y)$.

Definition 1.44. Let σ be a primitive representation of a place $\mathcal{P}$ of Σ.

1. The *order* of ζ at a plae $\mathcal{P}$ is $\mathrm{ord}_{\mathcal{P}}\zeta = \mathrm{ord}_t\sigma(\zeta)$.
2. If $\mathrm{ord}_{\mathcal{P}}\zeta = 1$ then ζ is a *local parameter* at $\mathcal{P}$.
3. The place $\mathcal{P}$ is a *zero* of *multiplicity* $\mathrm{ord}_{\mathcal{P}}\zeta$ if $\mathrm{ord}_{\mathcal{P}}\zeta > 0$.

4. The place $\mathcal{P}$ is a *pole* of *multiplicity* $-\mathrm{ord}_{\mathcal{P}}\zeta$ if $\mathrm{ord}_{\mathcal{P}}\zeta < 0$.

Theorem 1.45 (Theorem 5.33 of [9])**.** *The number of zeros counted with multiplicity is* $[\Sigma : K(\zeta)]$.

Corollary 1.46 (Corollary 5.35 of [9])**.** *The number of zeros and pole of* ζ *are equal, so*

$$\sum_{\mathcal{P}\in\mathfrak{P}(\Sigma)} ord_{\mathcal{P}}\zeta = 0.$$

Definition 1.47. Let $\zeta \in \Sigma$. For any $\eta \in \Sigma\backslash K$, the irreducible polynomial $f(X, Y)$ such that $f(\zeta, \eta) = 0$ has the property that $f(\zeta, Y) \in K(\zeta)[Y]$ is separable, then ζ is *separable*.

The derivation and differential copies from that of $K((t))$ and $K((t))dt$ to Σ.

Definition 1.48. We define the order of $d\zeta$ in the following way

$$\mathrm{ord}_{\mathcal{P}} d\zeta = \mathrm{ord}_t \frac{d\overline{\zeta}(t)}{dt}$$

where $\overline{\zeta}(t)$ denotes the image of ζ by a place representation corresponding to $\mathcal{P}$.

Theorem 1.49. *For a separable variable* ζ*, the genus* g *of* Σ *satisfies*

$$\sum_{\mathcal{P}\in\mathfrak{P}(\Sigma)} ord_{\mathcal{P}} d\zeta = 2g - 2$$

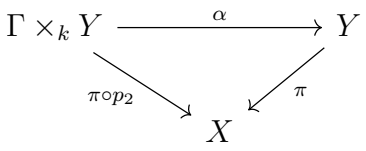
Definition 1.50. The *genus* of an irreducible algebraic curve is the genus of its function field Σ.

1.4 Principal Homogeneous Space

Let k be a field and X be a smooth k-scheme. Let Γ be an algebraic group over k.

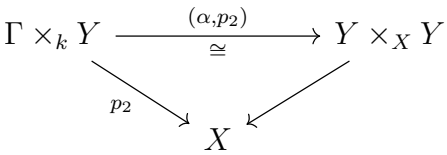
Definition 1.51. A *principal homogeneous space* (PHS in the sequel)for Γ over X is a surjective morphism $\pi : Y \to X$ such that

1. There exists an associative nontrivial action $\Gamma \times_k Y \xrightarrow{\alpha} Y$ such that the diagram commutes



and

2. There exsists an isomorphism



Chapter 2

Artin-Schreier cover

In this chapter we define a generalized Artin-Schreier cover over the thrice punctured plane X. For a group scheme Γ, which is constructed by an additive polynomial, generalized Artin-Schreier cover is defined as a principal homogeneous space of Γ. Depending on Γ being in the base ring or not, split or nonsplit cases are considered.

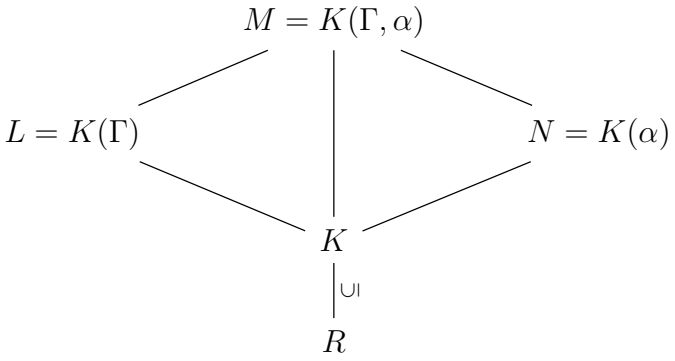
2.1 Generalized Artin-Schreier cover

The thrice punctured plane is defined as Spec R for the ring $R := k\Big[x, \frac{1}{x}, \frac{1}{1-x}\Big]$. Let $K = k(x)$ be the fraction field of R. Fix an separable algebraic closure $\overline{K}$ of K. Let $\Gamma \in \overline{K}$ be a finite R-additive subgroup, which implies that

$$f_\Gamma(T) = \prod_{\gamma \in \Gamma} (T - \gamma)$$

is a polynomial with coefficients in R. Let $L = K(\Gamma)$ be the field obtained by adjoining all elements of Γ to K. Then L/K is Galois because L is a splitting field of a separable polynomial $f_\Gamma(T)$ over K.

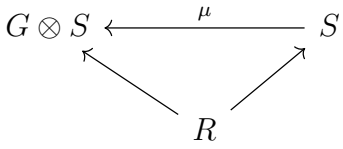
Choose $u \in K$ such that $f_\Gamma(T) - u \in K[T]$ is irreducible over both in K and L. Let $\alpha \in \overline{K}$ a root of $f_\Gamma(T) - u$. Define $M := L(\alpha) = K(\Gamma, \alpha)$ to be the field adjoining α to L. Then M/L and M/K are both Galois extension realized as a splitting field of a separable polynomial $f_\Gamma(T) - u$. Note that M, in general, is not isomorphic to a quotient field $N := K[T]/(f_\Gamma(T) - u)$. The following diagram shows the relations



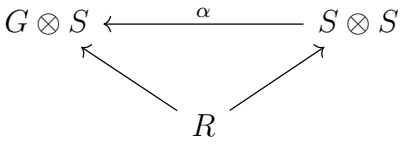
Let $X := \text{Spec } R$ and $\tilde{X} := \text{Spec } \Big(R[T]/(f_\Gamma(T) - u)\Big)$. The following notation for group scheme is not confusing in our context, so we use $\Gamma := \text{Spec } \Big(R[T]/(f_\Gamma(T))\Big)$. Write $S = R[T]/\langle f_\Gamma(T) - u\rangle$ and $G = R[T]/\langle f_\Gamma(T)\rangle$.

Theorem 2.1. *$\tilde{X}$ is a PHS of Γ over X.*

Proof. From the definition of PHS, the corresponding Hopf algebra diagrams are



and



Let $\bar{T}$ be the class of T in G and $\tilde{T}$ be the class of T in S. Define the map $\mu : S \to G \otimes S$ by $\tilde{T} \mapsto \bar{T} \otimes 1 + 1 \otimes \tilde{T}$. Note that $\tilde{T}$ in S satisfies $f_\Gamma(\tilde{T}) - u = 0$. Then

$$\begin{aligned}
\mu(f_\Gamma(\tilde{T}) - u) &= f_\Gamma(\bar{T} \otimes 1 + 1 \otimes \tilde{T}) - 1 \otimes u \\
&= f_\Gamma(\bar{T}) \otimes 1 + 1 \otimes \Big(f_\Gamma(\tilde{T}) - u\Big) \\
&= 0
\end{aligned}$$

Note that the map from $S \otimes S$ to $G \otimes S$ is determined by the map μ, which corresponds to the group action Γ on $\tilde{X}$ and the identity. Then the map is

given by

$$\begin{aligned}\alpha : K[\tilde{T}] \otimes_R K[\tilde{T}] &\longrightarrow K[\bar{T}] \otimes_R K[\tilde{T}] \\ \tilde{T} \otimes 1 &\longmapsto \bar{T} \otimes 1 - 1 \otimes \tilde{T} \\ 1 \otimes \tilde{T} &\longmapsto 1 \otimes \tilde{T}\end{aligned}$$

It needs to be verified that the image of the classes $\big(f_\Gamma(T) - u\big) \otimes 1$ and $1 \otimes \big(f_\Gamma(T) - u\big)$ is zero.

$$\begin{aligned}\alpha\Big(\big(f_\Gamma(\tilde{T}) - u\big) \otimes 1\Big) &= \alpha\Big(f_\Gamma(\tilde{T} \otimes 1 - 1 \otimes u\Big) \\ &= f_\Gamma(\bar{T} \otimes 1 - 1 \otimes \tilde{T}) - 1 \otimes u \\ &= f_\Gamma(\bar{T}) \otimes 1 - 1 \otimes \Big(f_\Gamma(\tilde{T}) - u\Big) \\ &= 0\end{aligned}$$

Therefore, since the diagrams commute in the Hopf algebra level, the orignal group scheme diagrams also commute. □

Definition 2.2. In the above contruction of generalized Artin-Schreier cover of the scheme X, if the K-additive subgroup Γ is a subset of R, then we call the cover $\tilde{X}$ is *split*.

Remark 2.3. Consider the affine scheme $R = \operatorname{Spec} k\Big[x, \dfrac{1}{x}, \dfrac{1}{1-x}\Big]$. Then the cover $\tilde{X}$ being split means that $L = K$, so the field M and N are equal, that is, the splitting field of $f_\Gamma(T) - u$ over K is same as the quotient field $N = K[T]/\langle f_\Gamma(T) - u\rangle$ and the group scheme Γ is discrete. Then the generalized Artin-Schreier cover is given by the Galois extension N/K whose Galois group is the additive subgroup isomorphic to Γ.

2.2 Function field arithmetic

In this section we take an example of generalized Artin-Schreier extension over a field and compute the genus of it. Let $f_\Gamma(T) = T^{p^n} + xT$ and $u = -x(x-1)$. Here, we consider the case when $p > 0$ is odd.

Let's compute the genus of the function field of the curve $\mathcal{F}$ which is

defined by the following equation:

$$f(X,Y) = Y^{p^n} - XY + X(X-1) \in k[X,Y].$$

Let's first check if $f(X,Y)$ has any singularities :

$$\frac{\partial f}{\partial X} = -Y + 2X - 1$$
$$\frac{\partial f}{\partial Y} = -X$$

To have a singular point, we have $X = 0$ and also $Y = 0$ because of $f(X,Y) = 0$. However, then the partial derivative $\partial f/\partial X$ is nonzero. So, there is no singular point on the affine plane.

Apply Proposition 1.19 to check the irreducibility of $f(X,Y)$. Consider $f(x,Y) = Y^{p^n} - xY - x(x-1) \in k(x)[Y]$ as a polynomial in Y over the rational function field $k(x)$. Apply the above theorem with the place $\mathcal{P} = \mathcal{P}_0$ of the funciton field K/k, we know that $f(x,Y)$ is irreudiclbe over K. This implies that $f(X,Y)$ is irreducible in $k[X,Y]$.

Let y be a root of $f(x,Y)$ and let $\Sigma = k(x,y)/k$ be the function field. Recall that the genus of the function field Σ satisfies

$$\sum_{\mathcal{P} \in \mathbb{P}_\Sigma} \mathrm{ord}_{\mathcal{P}} dx = 2g - 2.$$

To compute the genus, we classify the points on the curve $\mathcal{F}$ into 3 groups: points on affine plane with non-veritical tangent line, points on affine plane with vertical tangent line, and points at infinity.

1. **Points on affine plane with non-vertical tangent line.**

   According to Theorem 1.32 and Theorem 1.37, on a simple point of a plane curve $\mathcal{F}$, there exists a unique branch and the unique branch can be representedby the following :

   $$x(t) = u + t$$
   $$y(t) = v + \eta(t)$$

   with $\mathrm{ord}_t \eta(t) \geq 1$. Then for these points, $\mathrm{ord}_{\mathcal{P}} dx = 0$ and they have no contribution of the summation $\sum_{\mathcal{P} \in \mathbb{P}_\Sigma} \mathrm{ord}_{\mathcal{P}} dx$.

2. **Points on affine plane with vertical tangent line.**

   At a point (x_0, y_0) with a vertical tangent line, it satisfies $\dfrac{\partial f}{\partial Y}(x_0, y_0) = 0$. On $\mathcal{F}$, only $\mathcal{O} = (0,0)$ satisfies it and it is not singular. Then a primitive branch representation is

$$\begin{aligned} x(t) &= c_1 t^{i_1} + c_2 t^{i_2} + \ldots, \qquad \text{where } 0 < i_1 < i_2 < \cdots \\ y(t) &= t \end{aligned}$$

   Computing i_1 and i_2 explicitly, we have

$$\begin{aligned} f(x(t), y(t)) =& t^{p^n} - (c_1 t^{i_1} + c_2 t^{i_2} + \ldots)t \\ &+ (c_1 t^{i_1} + c_2 t^{i_2} + \ldots)(-1 + c_1 t^{i_1} + c_2 t^{i_2} + \ldots) \\ =& t^{p^n} - c_1 t^{i_1+1} - c_2 t^{i_2+1} - \ldots \\ &- c_1 t^{i_1} - c_2 t^{i_2} + c_1^2 t^{2i_1} + \ldots \\ =& 0 \end{aligned}$$

   This determines i_1, i_2 and so forth, where

$$i_1 = p^n \text{ and } i_2 = p^n + 1.$$

   Then

$$\operatorname{ord}_t \frac{dx(t)}{dt} = p^n.$$

3. **Points at infinity.**

   By homogenizing the curve $f(X, Y)$, we get

$$F(X, Y, Z) = Y^{p^n} - XYZ^{p^n-2} + X^2 Z^{p^n-2} - XZ^{p^n-1}$$

   and the partials are given by

$$\begin{aligned} \frac{\partial F}{\partial X} &= -YZ^{p^n-2} + 2Z^{p^n-2} - Z^{p^n-1} \\ \frac{\partial F}{\partial Y} &= -XZ^{p^n-2} \\ \frac{\partial F}{\partial Z} &= 2XYZ^{p^n-2} - 2X^2 Z^{p^n-2} + XZ^{p^n-2} \end{aligned}$$

   Then $X_\infty = (1:0:0)$ is the only point at inifinity and it is singular

with multiplicity $p^n - 2$. By setting $X = 1$, we get

$$g(Y, Z) = Y^{p^n} - YZ^{p^n-2} + Z^{p^n-2} - Z^{p^n-1}$$

Then $(0, 0)$ is a singular point with multiplicity $p^n - 2$ with only one tangent $\mathcal{V}(Z)$, the Y axis. Let $\mathcal{G}$ be the plane curve defined by $g(Y, Z)$.

Computing the primitive branch representation explicitly, we let

$$\begin{aligned} y(t) &= t^{i_1} + c_2 t^{i_2} + \ldots, && \text{where } i_1 < i_2 < \cdots \\ z(t) &= d_1 t^{j_1} + d_2 t^{j_2} + \ldots, && \text{where } j_1 < j_2 < \cdots \end{aligned}$$

with $\gcd(i_1, j_1) = 1$. Such pair (i_1, j_1) can be chosen due to Theorem 4.21 of [9]. Then it should satisfy

$$g(y(t), z(t)) = 0.$$

Explicitly plug in $y(t)$ and $z(t)$, we get

$$\begin{aligned} g(y(t), z(t)) =& (t^{i_1} + c_2 t^{i_2} + \ldots)^{p^n} - (t^{i_1} + c_2 t^{i_2} + \ldots)(d_1 t^{j_1} + d_2 t^{j_2} + \ldots)^{p^n-2} \\ &+ (d_1 t^{j_1} + d_2 t^{j_2} + \ldots)^{p^n-2} - (d_1 t^{j_1} + d_2 t^{j_2} + \ldots)^{p^n-1} \\ =& t^{i_1 p^n} + c_2^{p^n} t^{i_2 p^n} + \ldots \\ &- d_1^{p^n-2} t^{i_1 + j_1(p^n-2)} - d_1 c_2 t^{i_2 + j_1(p^n-2)} \\ &- \binom{p^n - 2}{1} d_1^{p^n-3} d_2 t^{i_1 + j_1(p^n-3) + j_2} + \ldots \\ &+ d_1^{p^n-2} t^{j_1(p^n-2)} + \binom{p^n - 2}{1} d_1^{p^n-3} d_2 t^{j_1(p^n-3)+j_2} + \ldots \\ &- d_1^{p^n-1} t^{j_1(p^n-1)} - \binom{p^n - 1}{1} d_1^{p^n-2} d_2 t^{j_1(p^n-2)+j_2} + \ldots \end{aligned}$$

Note that the last equality express the expansion of parenthesis upto

possible 2nd least degree terms. The list of degrees are

$$\begin{array}{lll} i_1p^n, & i_2p^n & \\ i_1 + j_1(p^n-2), & i_2 + j_1(p^n-2), & i_1 + j_1(p^n-3) + j_2 \\ j_1(p^n-2), & j_1(p^n-3) + j_2 & \\ j_1(p^n-1), & j_1(p^n-2) + j_2 & \end{array}$$

Since $g(y(t), z(t)) = 0$, we get $i_1p^n = j_1(p^n - 2)$ considering the least degree terms, where

$$i_1 = p^n - 2 \text{ and } j_1 = p^n.$$

If p was even, such i_1 and j_1 contradicts the condition $\gcd(i_1, j_1) \neq 1$.

Consider the 2nd least degrees, we get $i_1 + j_1(p^n - 2) = j_1(p^n - 3) + j_2$ and then

$$j_2 = 2p^n - 2$$

Then a branch representation of the curve $F(X, Y, Z)$ at X_∞ is given by

$$\begin{array}{ll} x(t) = 1 & \\ y(t) = t^{i_1} + c_2t^{i_2} + \ldots, & \text{where } i_1 = p^n - 2 < i_2 < \cdots \\ z(t) = d_1t^{j_1} + d_2t^{j_2} + \ldots, & \text{where } j_1 = p^n < j_2 = 2p^n - 2 < \cdots \end{array}$$

which is equivalent to

$$\begin{aligned} x(t) &= \frac{1}{d_1}t^{-j_1}\eta(t)^{-1} \\ y(t) &= \frac{1}{d_1}t^{i_1-j_1}\xi(t)/\eta(t) \\ z(t) &= 1 \end{aligned}$$

where

$$\eta(t) = 1 + \frac{d_2}{d_1}t^{j_2-j_1} + \frac{d_3}{d_1}t^{j_3-j_1} + \cdots$$

and $\xi(t) \in k((t))$ with $\mathrm{ord}_t \xi(t) = 0$. Then

$$\begin{aligned} x(t) &= \frac{1}{d_1} t^{-j_1} \eta(t)^{-1} \\ &= \frac{1}{d_1} t^{-j_1} (1 - \frac{d_2}{d_1} t^{j_2 - j_1} + \ldots) \\ &= \frac{1}{d_1} \Big(t^{-j_1} - \frac{d_2}{d_1} t^{j_2 - j_1} + \ldots \Big) \end{aligned}$$

and

$$\frac{dx(t)}{dt} = -\frac{1}{d_1} \cdot \frac{d_2}{d_1} (j_2 - 2j_1) t^{j_2 - 2j_1 - 1}$$

Then for each place γ of the curve $\mathcal{F}$ centered at $X_\infty = (1:0:0)$, we have

$$\mathrm{ord}_\gamma dx = j_2 - 2j_1 - 1 = 2p^n - 2 - 2p^n - 1 = -3.$$

Claim. The curve $\mathcal{F}$ has only one branch centered at $X_\infty = (1:0:0)$.

Proceed the argument on the affine plane $X = 1$. Let $\mathcal{G}$ and $g(Y, Z)$ be as before. Let $\mathcal{H}$ be the curve $\mathcal{V}(Y)$ and δ be a branch of $\mathcal{H}$ centered at $\mathcal{O} = (0, 0)$, which is represented by $y(t) = 0$ and $z(t) = t$. Then the intersection multiplicity of $\mathcal{G}$ with δ at $\mathcal{O} = (0, 0)$ is

$$I(\mathcal{O}, \mathcal{G} \cap \delta) = \mathrm{ord}_t(G(0, t)) = p^n - 2.$$

So, we have

$$I(\mathcal{O}, \mathcal{G} \cap \mathcal{H}) = p^n - 2$$

since $\mathcal{H}$ has only one branch δ.

Note that

$$\begin{aligned} p^n - 2 = I(\mathcal{O}, \mathcal{G} \cap \mathcal{H}) &= I(\mathcal{O}, \mathcal{H} \cap \mathcal{G}) \\ &= \sum_\gamma I(\mathcal{O}, \mathcal{H} \cap \gamma) \\ &= \sum_\gamma p^n - 2 \end{aligned}$$

where γ runs through all branches of $\mathcal{G}$ centered at P. Thus there is only one branch γ of $\mathcal{G}$ centered at $\mathcal{O}$.

Combining all three cases, from the equation

$$\sum_{\mathcal{P}\in\mathbb{P}_\Sigma} \mathrm{ord}_{\mathcal{P}} dx = 2g - 2$$

the only places contributing the summation on the left hand side is the one centered at $\mathcal{O}$ and $X_\infty = (1:0:0)$. Thus $p^n - 3 = 2g - 2$ and then

$$g = \frac{1}{2}(p^n - 1).$$

Remark 2.4. According to the genus computation, the thrice punctured plane have an abelian covering of arbitrary high genus for $p > 0$ odd.

Part II

Isometry-dual property of Algebraic Geometry Code

Chapter 3

Preliminaries

In this chapter, we review some definitions and properties of Algebraic Geometry Codes following the exposition of [12].

3.1 Codes

Let $\mathbb{F}_q$ be the finite field of q elements, where q is some power of a prime number p.

Definition 3.1. A *linear code* C is a linear subspace of $\mathbb{F}_q^n$. An element of C is a *codeword*. The *length* of C is n and the *dimension* of C is the dimension $\dim C$ as a $\mathbb{F}_q$-vector space.

We only discuss linear codes and we call them *codes* for short.

Definition 3.2. Let $\mathbf{a} = (a_1, \ldots, a_n)$ and $\mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$. The *Hamming distance* $d : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{R}$ is defined by

$$d(\mathbf{a}, \mathbf{b}) := |\{i : a_i \neq b_i\}|,$$

which counts the number of distinct components of $\mathbf{a}$ and $\mathbf{b}$. The *weight* is an integer valued function on $\mathbb{F}_q^n$ defined by

$$\mathrm{wt}(\mathbf{a}) := d(\mathbf{a}, \mathbf{0}).$$

The *minimum distance* of $C \neq 0$ is

$$d(C) := \min\{d(\mathbf{a}, \mathbf{b}) | \mathbf{a}, \mathbf{b} \in C \text{ and } \mathbf{a} \neq \mathbf{b}\} = \min\{\mathrm{wt}(\mathbf{c}) | \mathbf{0} \neq \mathbf{c} \in C\}$$

The full space $\mathbb{F}_q^n$ has structure as $\mathbb{F}_q$-algebra.

Definition 3.3. Let $\mathbf{a} = (a_1, \ldots, a_n)$ and $\mathbf{b} = (b_1, \ldots, b_n)$ be vectors in $\mathbb{F}_q^n$. An operation $* : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q^n$ is defined by

$$\mathbf{a} * \mathbf{b} = (a_1 b_1, a_2 b_2, \ldots, a_n b_n)$$

With this operation, an equivalence relation is defined on codes in $\mathbb{F}_q^n$.

Definition 3.4. Two codes C_1 and C_2 in $\mathbb{F}_q^n$ are said to be *equivalent* if there exists a vector $\mathbf{v} \in (\mathbb{F}_q^\times)^n$ such that $\mathbf{v} * C_1 = C_2$; i.e.,

$$C_2 = \{\mathbf{v} * \mathbf{a} \mid \mathbf{a} \in C_1\}.$$

3.2 AG code and its dual

Algebraic geometry codes, written by AG code in the sequel, were introduced by V. D. Goppa in [7] and are also called *geometric Goppa codes*. It is a linear code which is defined using the functions and rational points of a projective smooth curve over a field $\mathbb{F}_q$.

For the rest of the discussion, we use the following notations:

$\mathcal{X}$	smooth absolutely irreducible projective curve of genus g
$F = F(\mathcal{X})$	fucntion field of the curve $\mathcal{X}$
$P_1, \ldots, P_n, Q$	pairwise distinct rational points of $F/\mathbb{F}_q$
D	divisor given by $P_1 + \ldots + P_n$
G	divisor of $F/\mathbb{F}_q$ such that Supp $G \cap$ Supp $D = \emptyset$
$L(G)$	Riemann-Roch space of functions with $(f) \geq -G$

Consider the map defined on $L(G)$ as follows:

$$\begin{aligned} \mathrm{ev}_D : L(G) &\longrightarrow \mathbb{F}_q^n \\ f &\longmapsto (f(P_1), \cdots, f(P_n)). \end{aligned}$$

We often write the image of f by ev_D as $f(D)$.

Definition 3.5. An *AG code* $C_L(D, G)$ is a linear code given by the image of $L(G)$ by ev_D. If the divisor G is a multiple of Q, then $C_L(D, G)$ is called *one-point AG code*.

Definition 3.6. Two divisors G and H, both of which are disjoint from D, are said to be *rational equivalent* with respect to D, witten as $G \sim_D H$ if there exists a rational function u such that $u(P_i) = 1$ for all $i = 1, \ldots, n$ and $H = G + (u)$.

Now we define the dual of AG code which is given by residues of Weil differentials. Let $\Omega_F(G - D)$ be the Weil differential of $F/\mathbb{F}_q$.

Definition 3.7. The code $C_\Omega(D, G) \subseteq \mathbb{F}_q^n$ is defined by

$$\{(\mathrm{Res}_{P_1}(\omega), \ldots, \mathrm{Res}_{P_n}(\omega)) \mid \omega \in \Omega_F(G - D)\}$$

Theorem 3.8 (Theorem 2.2.7 of [12])**.** *The minimum distance d' of the code $C_\Omega(D, G)$ is given by*

$$d' \geq \deg G - (2g - 2).$$

The following theorem gives a relation between the two codes $C_L(D, G)$ and $C_\Omega(D, G)$.

Theorem 3.9 (Theorem 2.2.8 of [12])**.** $C_\Omega(D, G) = C_L(D, G)^\perp$

Next, we find a divisor H, by which the code $C_\Omega(D, G)$ is represented as $C_L(D, H)$. To this end, we need the following Lemma.

Lemma 3.10 (Lemma 2.2.9 of [12])**.** *There exists a Weil differential η such that*

$$v_{P_i}(\eta) = -1$$
$$Res_{P_i}(\eta) = 1 \text{ for } i = 1, \ldots, n$$

Proposition 3.11 (Proposition 2.2.10 of [12])**.** *Let η be the Weil differential given in Lemma 3.10. Then*

$$C_L(D, G)^\perp = C_\Omega(D, G) = C_L(D, H)$$

where $H := (\eta) + D - G$.

For a divisor G, we write $G^\perp := (\eta) + D - G$. Then the proposition shows that $C_L(D, G)^\perp = C_L(D, G^\perp)$.

For the rest of the section we give some statements will be needed to prove the Theorem 4.3 in the next chapter.

Lemma 3.12 (Lemma 3.1 of [10]). *Let C be a linear code in $\mathbb{F}_q^n$ not contained in any of the coordinate hyperplanes and $n < q$. Then there exits $\mathbf{c} \in C$ such that $wt(\mathbf{c}) = n$.*

Proof. Let C_i be the coordinate hyperplane defined by $x_i = 0$. Then $C \subsetneq C_i$ for all $i = 1, \ldots, n$. Suppose there is no codeword $\mathbf{c}$ in C of weight n. Then $C \subseteq \bigcup_{i=1}^{n} C_i$. Let $k = \dim C$. Counting the cardinality of both sets, we get $q^k \leq nq^{k-1}$, so $q \leq n$. This is a contradiction, so there is a codeword $\mathbf{c} \in C$ of weight n. □

Corollary 3.13 (Corollary 3.2 of [10]). *Let $n < q$ and $2g-1 < \deg G$. Then there exists a codeword of weight n in $C_L(D, G)$.*

Proof. If we can prove that the code $C_L(D, G)$ is not contained in any of the hyperplane x_i for $i = 1, \ldots, n$, then we are done. So, assume contrary that $C_L(D, G)$ is contained in some $x_i = 0$. Then its dual code $C_\Omega(D, G)$ contains a codeword of weight 1. However, the minimum distance of $C_\Omega(D, G)$ is at least $\deg G - (2g - 2)$, which is a contradiction. □

Viewing the curve $\mathcal{X}$ over the $\mathbb{F}_{q^r}$, the extension of $\mathbb{F}_q$,

Theorem 3.14 (Theorem 3.6.3 of [12]). *Consider the compositum of fields $F' := F\mathbb{F}_{q^r}$, then $F'/\mathbb{F}_{q^r}$ is an extension of the function field F/K. The conorm map*

$$Con_{F/F} : Cl(F) \longrightarrow Cl(F')$$

is injective.

Chapter 4

Isometry-dual property

Consider a full flag of codes in $\mathbb{F}_q^n$. If the flag is the same as its dual flag upto equivalence with respect to a fixed vector $\mathbf{v}$ with $\mathrm{wt}(\mathbf{v}) = n$, it is said to be isometry-dual. For one-point AG codes, by [6], the isometry-dual property can be characterized in two ways: one in terms of divisors and the other in terms of the Weierstrass semigroup of nongap numbers. In addition, interests are in the case when the isometry-dual property is preserved after puncturing the codes at some points. The paper [2] gives a necessary condition for a punctured flag of one-point AG codes preserving the isometry-dual property. In this chapter, after going through the detail of previous works, we generalize a result in [6] and give a different proof. Our proof does not depend on results in [10] that are used in the proof in [6] and in this way we are able to obtain a stronger result. Moreover, we present examples that show that our result are best possible. A further aspect of our proof is that it makes clear which part of the isometry-dual property of AG codes depends on curve properties and which part on linear algebra.

4.1 Isometry-dual property of one-point AG codes

In this chapter, we consider a full flag $(C_i)_{i=0,\dots,n}$ of codes, that is, a series of codes with strict inclusions

$$\{0\} = C_0 \subsetneq C_1 \subsetneq \dots \subsetneq C_n = \mathbb{F}_q^n$$

such that $\dim C_i = i$.

Definition 4.1. The full flag $(C_i)_{i=0,\dots,n}$ is *isometry-dual* if there exists a

vector $\mathbf{v} \in (\mathbb{F}_q^\times)^n$ such that

$$C_i \perp_{\mathbf{v}} C_{n-i},$$

or, equivalently, if the dual flag

$$\mathbb{F}_q^n = C_0^\perp \supsetneq C_1^\perp \supsetneq \ldots \supsetneq C_n = \mathbb{F}_{q^n}^\perp = \{0\}$$

is the same as the original flag modulo the equivalence with respect to $\mathbf{v}$. Note that the vector $\mathbf{v}$ depends on the flag $(C_i)_{i=0,\ldots,n}$ but not on i.

Consider one-point AG codes on a smooth absolutely irreducible projective curve $\mathcal{X}$ with genus g. Let W be the set of Weierstrass nongap numbers at a rational point Q. Let C_i be given by $C_L(D, m_i Q)$ with m_i satisfying the following:

1. $m_0 = -1$.
2. $\dim C_L(D, m_i Q) = i$ and m_i is minimal with respect to this property for $i = 1, \ldots, n$.

We call m_i a *geometric nongap* for each $i = 1, \ldots, n$ and let W^* be the set of all geometric nongaps. It is obvious that $W^* \subseteq W$. Then we have the following characterization of the full flag of one-point AG codes being isometry-dual.

Theorem 4.2 (Proposition 4.3 of [6]). *Suppose $n > 2g + 2$. Then the following are equivalent for the full flag $(C_L(D, m_i Q))_{i=0,\ldots,n}$.*

(a) The flag is isometry-dual.

(b) $(n + 2g - 2)Q - D$ is a canonical divisor.

(c) $n + 2g - 1 \in W^*$

where K is a canonical divisor.

The above theorem refers in its proof to the following theorem from [10], from which the condition $n > 2g + 2$ originated.

Theorem 4.3 (Theorem 4.14 and Corollary 4.15 of [10]). *Suppose $n > 2g+2$. Let G and H be divisors with supports disjoint from D. Let $2g-1 < \deg G = \deg H < n - 1$. Then $C_L(D, G) = C_L(D, H)$ if and only if $G \sim_D H$, i.e. there is a function f with $(f) = G - H$ and $f(P) = 1$ for all $P \in D$.*

Let I be an index set given as a subet of $\{1, 2, \ldots, N\}$ of size n. Consider a projection map $\mathrm{pr}_I : \mathbb{F}_q^N \to \mathbb{F}_q^n$ given by $\mathrm{pr}_I(\mathbf{c}) = (c_i)_{i \in I}$ for $\mathbf{c} \in \mathbb{F}_q^N$. For a code $C \subseteq \mathbb{F}_q^N$, we call $\mathrm{pr}_I(C) \subseteq \mathbb{F}_q^n$ the *punctured code* of C at positions $\{1, 2, \ldots, N\} \backslash I$. In one-point AG codes, we can define it in the following way.

Definition 4.4. For one-poin AG code $C_L(D, mQ)$, the *punctured* code at points $P_{i_1}, \ldots P_{i_l}$ is $C_L(D', mQ)$ where $D - D' = P_{i_1} + \ldots + P_{i_l}$.

For a full flag of one-point AG codes $(C_L(D, m_iQ))_{i=0,\ldots,N}$, the puncturing will induce a new series of codes $(C_L(D', m_iQ))_{i=0,\ldots,N}$. Note that there are some redundancies in the series since the length of the flag is N but the codes are in $\mathbb{F}_q^n$ if $n < N$. So, we remove $C_L(D', m_iQ)$ from the series if it satisfies

$$C_L(D', m_iQ) = C_L(D', m_{i-1}Q).$$

In this way, we get a full flag of length n after puncturing. We can formulate it in more strict sense.

Definition 4.5. Let $D' \subset D$ be a divisor with $|D'| = n$. For a full flag of one-point AG codes $(C_L(D, m_iQ))_{i=0,\ldots,N}$, the punctured flag at points $D - D'$ gives a full flag $(C_L(D', m_i'Q))_{i=0,\ldots,n}$ where the subset $\{m_0', m_1', \ldots, m_n'\} \subseteq \{m_0, m_1, \ldots, m_N\}$ are chosen to satisfy $C_L(D', m_i'Q) \neq C_L(D', (m_s - 1)Q)$. The m_i' satisfying the last condition are called *optimal*.

In [2], for one-point AG codes, a necessary condition is given for the inheritance of the isometry-dual property from the original flag to its punctured flag.

Theorem 4.6 (Theorem 6 of [2])**.** *Suppose $N \geq n > 2g + 2$. Let a full flag of one-point AG codes $(C_L(D, m_iQ)_{i=0,\ldots,N}$ be isometry-dual. Consider a full flag codes $(C_L(D', m_i'Q))_{i=0,\ldots,n}$ obtained by puncturing at $D - D'$. The flag of punctured codes is also isometry-dual only if $N - n \in W$, i.e., only if $L((N-n)Q) \neq L((N-n-1)Q)$.*

It will be shown in the next section that the proof of the equivalence of (a) and (c) in Theorem 4.2 depends highly on (b). Here we present a generalization and a different proof. In this way, we can see what aspect of a curve contributes to the isometry-dual property and its inheritance to a puncturing.

Theorem 4.7. *Let $C_L(D, m_iQ)_{i=0,\dots,N}$ be a full flag of one-point AG codes. For a divisor $D' \subset D$, suppose that the punctured flag $C_L(D', m'_i)_{i=0,\dots,n}$ is isometry-dual. Let $m := m'_n$. Then only one of the following three can occur.*

(a) If $m \geq 4g$, then $n = m - 2g + 1$.

(b) If $m \leq 4g - 2$, then $n \leq 2g$.

(c) If $m = 4g - 1$, then either $n = 2g$ or $n = 2g + 1$.

Note that, in the above theorem, we do not exclude the case $n = N$. So, the theorem can be used to see if the original flag is isometry-dual.

Remark 4.8. If $n = 2g + 2$ then $m = n + 2g - 1$. So the equivalence of (a) and (c) in Theorem 4.2 can be extended to the case $n = 2g + 2$. It can be shown easily that (c) implies (a).

In the rest of this section we will prove Theorem 4.3, Theorem 4.2, and Theorem 4.6.

4.1.1 Equivalence of divisors from equality of codes

In [10], the complete proof of Theorem 4.3 spreads out in many Theorems and Corollaries combined with more general cases. In this subsection we give compact and essential proof of the theorem extracted from [10]. Throughout this subsection let G and H be two divisors with same degree m. For notation, we write $m^\perp := n + 2g - 2 - m$.

The following are some preliminary works which will be needed in the proof of the Theorem 4.2.

Remark 4.9 (Remark 4.4 of [10]). The following fact can be verified readily from the definition of $G^\perp$.

$$\begin{aligned} G^\perp \cap H^\perp &= D + K - G - H + G \cap H \\ &= G^\perp + H^\perp - D - K + G \cap H \end{aligned}$$

Remark 4.10 (Proposition 4.5 of [10]). Let E and F be two divisors with $\ell(F) \neq 0$. Suppose $2g - 1 < \deg F$ and $\deg E < \deg F$. Then $\ell(E) < \ell(F)$. Indeed, if $\deg E \leq 2g - 2$, then by Clifford's theorem and Riemann-Roch theorem, we get $\ell(E) \leq g < \ell(F)$. If $\deg E > 2g - 2$, then also by Riemann-Roch theorem, $\ell(E) < \ell(F)$.

The proof of the following proposition refers to [4].

Proposition 4.11 (Proposition 4.7 of [10]). *Let G and H be two divisors with $\deg G = \deg H = m$, both of which are not supported in D. If $2g-1 < m < n-1$ and $C_L(D,G) = C_L(D,H)$ then*

$$\ell(G) \leq \ell(G \cap H) + \ell(G + H - G \cap H - D).$$

Proof. For any $f \in L(G)$, let $h_f \in L(H)$ be such that $\mathrm{ev}_D(f) = \mathrm{ev}_D(h_f)$. The function h_f is unique because if $\mathrm{ev}_D(f) = \mathrm{ev}_D(h_f) = \mathrm{ev}_D(h'_f)$, then $h_f - h'_f \in L(H - D) = \{0\}$. Consider the map

$$\begin{aligned} \phi : L(G) &\longrightarrow F(\mathcal{X}) \\ f &\longmapsto h - h_f \end{aligned}$$

Let V be the image of ϕ. Then $\ker \phi = L(G \cap H)$. Note that $V \simeq L(G)/L(G \cap H)$, so $\ell(G) = \dim V + \ell(G \cap H)$. If $f \in L(G)$ and $h \in L(H)$ then $f - h \in L(G + H - G \cap H)$. Since the image of ϕ vanishes at all D, we get $\dim V \leq \ell(G + H - G \cap H - D)$. Therefore we get the result. □

Lemma 4.12 (Lemma 4.10 of [10]). *Let $2g-1 < m < n-1$. Suppose $0 \leq \deg(G \cap H) \leq 2g-2$ and $0 \leq \deg(G + H - G \cap H - D) \leq 2g-2$. If $C_L(D,G) = C_L(D,H)$ then $n \leq 2g+2$.*

Proof. Note that $\ell(G) = m+1-g$. Applying Proposition 4.11 and Clifford's theorem, we get

$$\begin{aligned} m+1-g &\leq \Big(\frac{\deg(G \cap H)}{2} + 1\Big) + \Big(\frac{\deg(G + H - G \cap H - D)}{2} + 1\Big) \\ &= m - \frac{n}{2} + 2 \end{aligned}$$

Then $n \leq 2g+2$. □

Proof of Theorem 4.3. The proof is given in three steps starting with some restrictions on the degrees of G and H and then removing the restrictions as the proof proceeds.

Step 1. The theorem holds with an additional condition $\deg(G \cap H) > m - n$.

Let $s := \deg(G \cap H)$ and $t := \deg(G^\perp \cap H^\perp)$. We will use the following relation, which can be readily obtained from the definition.

$$\begin{aligned}\deg(G + H - G \cap H - D) &= 2m - n - s \\ &= \deg((\eta) - G^\perp \cap H^\perp) = 2g - 2 - t\end{aligned}$$

We prove separately for cases for s and t.

(a) $s > 2g - 2$

$\deg(G^\perp \cap H^\perp) = 2m^\perp - n - (2g-2) + s > 2m^\perp - n$ by Remark 4.9. If $G^\perp \neq H^\perp$ then

$$G^\perp \cap H^\perp < G^\perp$$

so $\deg(G^\perp \cap H^\perp) < \deg G^\perp$. By Lemma 4.11, we get $\ell(G^\perp \cap H^\perp) < \ell(G^\perp)$. Applying Lemma 4.12, we get

$$\begin{aligned}\ell(G^\perp \cap H^\perp) < \ell(G^\perp) &< \ell(G^\perp \cap H^\perp) + \ell(G^\perp + H^\perp - G^\perp \cap H^\perp - D) \\ &= \ell(G^\perp \cap H^\perp),\end{aligned}$$

which is a contradiction. Therefore $G^\perp = H^\perp$, so $G = H$.

(b) $t > 2g - 2$

The argument is same if we replace G, H, and s by $G^\perp$, $H^\perp$, and t respectively.

(c) $0 \leq s \leq 2g - 2$

Note that

$$0 \leq \deg(G + H - G \cap H - D) = \deg((\eta) - G^\perp \cap H^\perp) \leq 2g - 2.$$

Then by Lemma 4.12, this implies that $n \leq 2g + 2$, which contradicts the assumption $n > 2g + 2$. So, this case does not occur.

(d) $0 \leq t \leq 2g - 2$

The argument is same if we replace G, H and s by $G^\perp$, $H^\perp$, and t respectively.

(e) $s < 0$

Note that $\ell(G \cap H) = 0$. Then $\ell(G) \leq \ell(G + H - G \cap H - D)$ by

Proposition 4.11. Since $m - n < s$ from the assumption, we get

$$\deg(G + H - G \cap H - D) < \deg G.$$

Applying Remark 4.10 for $E = G + H - G \cap H - D$ and $F = G$, it has to be that

$$\ell(G + H - G \cap H - D) < \ell(G),$$

which is a contradiction. So, this does not occur.

(f) $t < 0$

The argument is similar to (e) after replacing G, H, and s by $G^{\perp}$, $H^{\perp}$, and t respectively.

Therefore we get the following table of cases for the degree of s and t, wihch proves the Theorem with additional condition $\deg(G \cap H) > m - n$.

	$s > 2g-2$	$0 \le s \le 2g-2$	$s < 0$
$t > 2g-2$	(a), (b)	(d)	(e)
$0 \le t \le 2g-2$	(c)	(c),(d)	(e)
$t < 0$	(f)	(f)	(e),(f)

The cases corresponding to shaded regions does not occur. Note that with the additional assumption $\deg(G \cap H) > m - n$, we proved $G = H$.

Step 2. The theorem holds if both G and H are effective.

Since $\deg(G \cap H) \ge 0 > m - n$, it is a special case of Step 1.

Step 3. The theorem holds for general G and H.

View the codes $C_L(D, G)$ and $C_L(D, H)$ in $\mathbb{F}_{q^r}^n$ for some r large enough to satisfy $q^r > n$. According to Corollary 3.13, there exist $f \in L(G)$

and $h \in L(H)$ be such that $\mathrm{ev}_D(f) = \mathrm{ev}_D(h)$ with weight n. Let $G' = G + (f)$ and $H' = H + (h)$. Then G' and H' are both effective and $\mathrm{ev}_D(f) * C_L(D, G') = C_L(D, G) = C_L(D, H) = \mathrm{ev}_D(h) * C_L(D, H')$. Then $G' = H'$ by Step 2. Therefoer $G \sim_D H$. By Theorem 3.14, equivalence of G and H over $\mathbb{F}_{q^r}$ implies the equivalnece of G and H over $\mathbb{F}_q$.

□

4.1.2 Isometry-dual property in two characterizations

In this subsection we give proof of Theorem 4.2.

Lemma 4.13. *Let $A = m_i Q$ and $B = m_j Q$ be divisors given by multples of Q. If $A + B \sim K + D + Q$ for a canonical divisor K then*

$$m_i \in W^* \Leftrightarrow m_j \in W^*$$

Proof. Suppose that $m_i \in W^*$, then

$$L(A)/L(A - D) \cong L(K + D + Q - B)/L(K + Q - B)$$
$$\dim L(A)/L(A - D) - \dim L(A - Q)/L(A - Q - D) = 1$$

Combining the above two facts, we get

$$\dim L(K + D + Q - B)/L(K + Q - B) - \dim L(K + D - B)/L(K - B) = 1$$

Applying the Riemann-Roch Theorem, we get

$$\dim L(B)/L(B - D) - \dim L(B - Q)/L(B - Q - D) = 1$$

Thus we conclude that $m_j \in W^*$. The converse can be shown similarily. □

Proof of Theorem 4.2. Let E be the divisor $(n + 2g - 2)Q - D$.

(a) ⇒ (b) Assume that the sequence $(C_L(D, m_i Q))_{i=0,\cdots,n}$ is isometry-dual. Choose i such that $2g \leq m_i \leq n - 1$. This is possible since $2g + 2 < n$ and there is no Weierstrass gap number of Q between $2g$ and n. Since

$2g \leq n+2g-2-m_i \leq n-1$, there exists j such that $m_j = n+2g-1-m_i$, where $m_j \in W^*$. From the isometry-dual property, we get

$$C_L(D, m_iQ) \perp_f C_L(D, m_{n-i}Q)$$

and for K is cacnonical

$$C_L(D, m_iQ)^\perp = C_L(D, K + D - m_iQ).$$

Let's first show that $i + j = n$. Using Riemann-Roch theorem, we get the following.

$$\begin{aligned} \dim C_L(D, m_iQ) &= n - \ell(K + D - m_iQ) = i \\ &= \ell(m_iQ) = m_i + 1 - g = i \end{aligned}$$

Similarly, $j = m_j + 1 - g$ and then

$$i + j = m_i + m_j - 2g + 2 = n$$

Thus

$$C_L(D, K + D - m_iQ) \sim C_L(D, m_jQ).$$

By Theorem 4.3, it will be induced that $K + D - m_iQ \sim m_jQ$ and then the divisor $(n + 2g - 2)Q - D$ is canonical.

(b) $\Rightarrow$ (a) First, assume that $(\omega) = (n + 2g - 2)Q - D$ is a canonical divisor. Let η be a differential as in Lemma 3.10. Choose f such that $f\omega = \eta$. Then f has no zero at P_i for $i = 1, \ldots, n$. Let $A = m_iQ$ and $B = (n + 2g - 1 - m_i)Q$ be divisors. Then

$$A + B = (n + 2g - 1)Q = (\omega) + D + Q \sim (\eta) + D + Q.$$

By the above Lemma 4.13, since $m_i \in W^*$, we have $n+2g-1-m_i \in W^*$, and

$$\begin{aligned} C_L(D, m_iQ)^\perp &= C_L(D, (\eta) + D - m_iQ) \\ &= C_L(D, (f) + (\omega) + D - m_iQ) \\ &= \mathrm{ev}_D(f) * C_L(D, (n + 2g - 2 - m_i)Q) \end{aligned}$$

with $\dim C_L(D,(n+2g-2-m_i)Q) = n-i$. Note that the first equality holds by Proposition 3.11 and the second is by $f\omega = \eta$. Thus $m_{n-i} = n+2g-2-m_i$ and $C_L(D,m_iQ) \perp_f C_L(D,m_{n-i}Q)$.

(b) $\Leftrightarrow$ (c) By the equivalence of (a) and (b), the flag is isometry-dual if and only if the divisor $A = (n+2g-2)Q - D$ is canonical. Note that $\deg A = 2g-2$. Then A is canonical if and only if $\ell(A) \geq g$ (See [12], Proposition 1.6.2). By Riemann-Roch theorem, $\ell(A+Q) = g$. Thus A is canonical if and only if $\ell(A) = \ell(A+Q)$. This is if and only if $n+2g-1 \in W^*$ due to the characterization of geometric nongaps.

Note that $\deg E = 2g-2$. Thus E is canonical if and only if $\ell(E) = g$. By Reimann-Roch theorem, $\ell(E+Q) = g$. Then E is canonical if and only if $\ell(E) = \ell(E+Q)$, which is equivalent to $n+2g-1 \in W^*$.

□

4.1.3 Maximal sparse ideal and inheritance of isometry-dual property

In this subsection we introduce the concept of maximal sparse ideal of a numerical semigroup and use it to prove Theorem 4.6. The exposition and result is from [2].

A *numerical semigroup* S is a subset of $\mathbb{N}_0$ which contains 0, is closed under addition and has a finite complement in $\mathbb{N}_0$. Write it as

$$S = \{0 = \lambda_0 < \lambda_1 < \lambda_2 < \cdots\} \subseteq \mathbb{N}_0.$$

Define $g := |\mathbb{N}_0 \backslash S|$ the *genus* and $c := \min\{i : i + \mathbb{N}_0 \subseteq S\}$ the *conductor* of S. In [1], a partial order $\preceq$ on a numerical semigroup S is defined as follow

$$\lambda_i \preceq \lambda_j \iff \exists \lambda_k \in S \text{ such that } \lambda_i + \lambda_k = \lambda_j$$

With the definition define the following two sets for any $\lambda_i \in S$.

$$D(\lambda_i) := \{\lambda_j \in S : \lambda_j \preceq \lambda_i\}$$
$$\Gamma(\lambda_i) := \{\lambda_j \in S : \lambda_i \preceq \lambda_j\}$$

A proper subset I is an *ideal* of S if $I + S \subseteq I$. An ideal I is *irreducible* if it is not an intersection of two ideals properly containing I. The *Frobenius number* F of an ideal I is the largest number not in I.

Remark 4.14. Here, we list series of facts whose proof can be found in [2].

1. $\Gamma(\lambda_i)$ is an ideal of S.
2. All irreducible ideals are of the form $S\backslash D(\lambda_i)$ for some λ_i and all set of such form are irreducible.
3. $F \leq 2g - 1 + |S\backslash I|$ and we call an ideal I *maximum sparse* if the equality holds.

Let $g(\lambda_i)$ denote the number of pairs of gaps adding to λ_i. Then the following holds.

Theorem 4.15 (Theorem 4 of [2]). *Let I and J be two maximum sparse ideal of S with corresponding leaders λ_i and λ_j respectively. Then the following are equivalent:*

(1) $J \supseteq I$

(2) $S\backslash J \subseteq S\backslash I$

(3) $D(\lambda_j) \subseteq D(\lambda_i)$

(4) $\lambda_i - \lambda_j \in S$

(5) $|S\backslash I| - |S\backslash J| \in S$

Theorem 4.16 (Theorem 2 of [3]). *An ideal I of S is maximum sparse if and only if $I = S\backslash D(\lambda_i)$ for some i and $g(\lambda_i) = 0$.*

Consider the one-point AG codes setting with the Weierstrass semigroup W and geometric nongaps W^*.

Proposition 4.17 (Corollary 3.3 of [6]). *The set $W\backslash W^*$ is an ideal of W.*

Remark 4.18. Note that $n + 2g - 1 \in W^*$ is equivalent to $W\backslash W^*$ being maximum sparse. Indeed, if $n+2g-1 \in W^*$, it is maximum in W^* due to the dimension argument of $C_L(D, (n + 2g - 1)Q)$ using Reimann-Roch theorem. Then $F = n + 2g - 1$ and $|W\backslash(W\backslash W^*)| = |W^*| = n$. Conversely, the ideal $W\backslash W^*$ being maximum sparse implies that $F = 2g - 1 + |W^*| = n + 2g - 1$. Then $F \in W^*$.

Proof of Theorem 4.6. Write (C_i) for the original flag and (C'_i) for the induced punctured flag. Assume that they are both isometry-dual. Let $(W^*)'$ be the set of geometric nongaps for the punctured flag. By the above remark, since both the orignal and the induced flags are isometry-dual, the ideal $W\backslash W^*$ and $W\backslash(W^*)'$ are both maximum sparse. For a fixed m, if $C'_m \neq C'_{m-1}$ then $C_m \neq C_{m-1}$. This implies $(W^*)' \subseteq W^*$. By Theorem 4.15, it is equivalent to $|W^*| - |(W^*)'| = n - s \in W$. □

4.2 Linear algebra argument

For a full flag of codes $(C_i)_{i=0,\dots,N}$, the isometry-dual property is defined only in terms of their inclusion of its dual flag modulo equivalence. So, we can extend it to general linear code, not necessarily induced from a curve.

Definition 4.19. Let A be a $N \times N$ matrix over $\mathbb{F}_q$ of rank N. The matrix A is *isometry-dual* if there exists a vector $\mathbf{v} \in (\mathbb{F}_q^\times)^N$ such that the matrix $A \cdot \mathrm{diag}(\mathbf{v}) \cdot A^T$ is a anti-diagonal lower triangular matrix with nonzero anti-diagonal components, i.e.

$$A \cdot V \cdot A^t = \begin{pmatrix} & & & & \star \\ & 0 & & \star & \\ & & \iddots & & \\ & \star & & * & \\ \star & & & & \end{pmatrix}$$

where all the anti-diagonal components, i.e. all $\star$, are nonzero. We call $\mathbf{v}$ a *dualizing vector*.

To easily move back and forth between linear algebra and AG codes, we define formal notions of points and functions of a matrix A.

Definition 4.20. Let A be an $N \times N$ matrix. Corresponding to each j-th column of A, we call P_j a point of A for $j = 1, \dots, N$. Write D for the set of all points of A ordered by i.

Definition 4.21. For each i-th row of A, corresponds f_i a *function* defined on points of A whose value at P_j is the (i, j) component of A. Define F to be a $\mathbb{F}_q$-algebra spanned by $f_1, \dots, f_n$ and call it a *function space* of A.

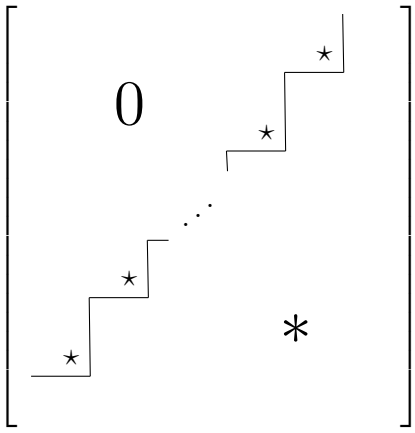
For a function f and the set of points D of a matrix A, We interchangeably write $\mathrm{ev}_D(f)$ or $f(D)$ for the row vector $(f(P_1), \ldots, f(P_N))$.

Puncturing a flag of codes corresponds to taking a $n \times n$ minor, say B, of the matrix A. Without loss of generality, by reordering columns if necessary, we may assume that the points $D' := \{P_1, \ldots, P_n\}$ are chosen for the minor B. For rows, let $\{b_1, \ldots, b_n\}$ be the rows chosen for the minor B, that is, the functions $\{f_{b_1}, \ldots, f_{b_n}\}$ be chosen. However, there is a restriction in choosing rows for B.

Definition 4.22. The $n \times n$ minor B of A is called *optimal* if the following hold. b_i has the property that $f_{b_i}(D')$ is linearly independent over $\{f_j(D') : j < b_i\}$.

Remark 4.23. Note that all definitions given above correspond to the definition for one-pont AG codes.

Proposition 4.24. *Let A be an $N \times N$ matrix of full rank. A $n \times n$ minor B of A is optimal and isometry-dual if and only if there exists a vector $\mathbf{w} \in \mathbb{F}_q^N$ with $wt(\mathbf{w}) = n$ such that $A \cdot \mathrm{diag}(\mathbf{w}) \cdot A^t$ is of the following form*



where the following hold:

1. *There are exactly n number of $\star$.*
2. *All $\star$ are nonzero.*
3. *Any component located left and/or above the $\star$ is zero.*

In a matrix of such form, we call a position of $\star$ a pivot. The vector $\mathbf{w}$ is called the characteristic vector.

Proof. First, we prove the if part. Suppose that there exists a vector $\mathbf{w} \in \mathbb{F}_q^N$ of weight n which makes the matrix $A \cdot \mathrm{diag}(\mathbf{w}) \cdot A^t$ of the required form. write $\mathbf{w} = (w_1, \ldots, w_N)$. Define $x_1 < x_2 < \cdots < x_n$ be the position of nonzero components of $\mathbf{w}$. If (x, y) is the position of a pivot, then the corresponding $\star$ is given by

$$(f_x(D) * \mathbf{w}) \cdot f_y(D).$$

Note that if (x, y) is a pivot position then so is (y, x). Let $(x_1, y_1), \ldots, (x_n, y_n)$ be the pivot positions, where x_i is in increasing order with respect to i. Let $D' = \{P_{b_1}, P_{b_2}, \ldots, P_{b_n}\}$ and consider the functions f_{x_i} for $i = 1, \ldots, n$. Then define

$$B = \left(f_{x_i}(P_{b_j})\right)_{1 \le i,j \le n}.$$

We claim that B is an optimal minor of A and that B is an isometry-dual matrix with dualizing vector $\mathbf{v}_B := (w_{b_1}, \ldots, w_{b_n})$. To show that it is optimal, we need to prove that $f_{x_i}(D')$ is linearly independent of all $f_j(D')$ for $j < x_i$. Suppose that $f_{x_i}(D')$ is linearly dependent, so can be expressed as

$$f_{x_i}(D') = \sum_{j < x_i} a_j f_j(D').$$

Then $(f_{x_i}(D') * \mathbf{v}_B) \cdot f_{y_i}(D') = \sum_{j<x_i} a_j (f_j(D) * \mathbf{w}) \cdot f_{y_i}(D) = 0$ since all $(f_j(D) * \mathbf{w}) \cdot f_{y_i}(D) = 0$ for $j < x_i$ because they are components located left of the $\star$ at (x_i, y_i). Thus $\star = 0$, which is a contradiction. This shows that the minor B is optimal.

In remains to prove that B is isometry-dual with respect to the vector $\mathbf{v}_B$. Any anti-diagonal component of $B \cdot \mathrm{diag}(\mathbf{v}_B) \cdot B^t$ is given as

$$(f_{x_i}(D') * \mathbf{v}_B) \cdot f_{y_i}(D') = (f_{x_i}(D) * \mathbf{w}) \cdot f_{y_i}(D) = \star$$

So, they are all nonzero. Components of $B \cdot \mathrm{diag}(\mathbf{v}_B) \cdot B^t$ above the anti-diagonal positions are

$$(f_{x_i}(D') * \mathbf{v}_B) \cdot f_{y_j}(D') = (f_{x_i}(D) * \mathbf{w}) \cdot f_{y_j}(D)$$

for $i < j$. Since the right hand side corresponds to values of $A \cdot \mathrm{diag}(\mathbf{w}) \cdot A^t$, located above of a pivot position, it is zero. This proves $B \cdot \mathbf{v}_B \cdot B^t$ is anti-diagonal lower triangular, so B is isometry-dual.

To prove the opposite direction, assume that the matrix B is isometry-dual. Then there is a vector $\mathbf{v}_B \in (\mathbf{F}_q^\times)^n$ such that $B \cdot \mathbf{v}_B \cdot B^t$ is anti-diagonal lower triangular. Write $\mathbf{v}_B = (v_1, v_2, \ldots, v_n)$. Let $D' := \{P_{b_1}, \ldots, P_{b_n}\} \subseteq D$ be the points corresponding to the columns of B with induced order from D and let $\{f_{x_1}, \ldots, f_{x_n}\}$ be the functions corresponding to the rows of B chosen from A with x_i increasing order with respect to i. Define $y_i := x_{n-i}$, for $i = 1, \ldots, n$, the order reversing of x_i's. Let a vector $\mathbf{w} \in \mathbb{F}_q^N$ have all zero components except b_i-th position, which is v_i for $i = 1, \ldots, n$. We need to prove that the matrix $A \cdot \mathrm{diag}(\mathbf{w}) \cdot A^t$ is of the required form. To this end, prove the following two claims.

1. The (x_i, y_i) components are nonzero for all $i = 1, \ldots, n$.

2. Any components located left and/or above the (x_i, y_i) position are zero.

Note that

$$(f_{x_i}(D) * \mathbf{w}) \cdot f_{y_i}(D) = (f_{x_i}(D') * \mathbf{v}_B) \cdot f_{y_i}(D') = \star \neq 0$$

since the second term is the value of the anti-diagonal components of $B \cdot \mathrm{diag}(\mathbf{v}_B) \cdot B^t$. This proves the first claim. Consider the (x, y) component of $A \cdot \mathrm{diag}(\mathbf{w}) \cdot A^t$ where $x \leq x_i$ and $y \leq y_i$ but $(x, y) \neq (x_i, y_i)$ for some i. We will show that $(f_x(D) * \mathbf{w}) \cdot f_y(D) = 0$.

(1) If $x < x_i$, then $f_x(D')$ is a linear combination of $f_{x_j}(D')$ for $j < i$ and $f_y(D')$ is a linear combination of $f_{y_k}(D')$ for $k \leq i$. Then $(f_x(D) * \mathbf{w}) \cdot f_y(D)$ is a linear combination of

$$(f_{x_j}(D) * \mathbf{w} \cdot f_{y_k}(D) = (f_{x_j}(D') * \mathbf{v}_B) \cdot f_{y_k}(D')$$

for $j < i$ and $k \leq i$. These are above the anti-diagonal components of $B \cdot \mathrm{diag}(\mathbf{w}) \cdot B^t$, so they are zero.

(2) If $y < y_i$, then it holds similarly.

Therefore there are exactly m pivot positions in the matrix $A \cdot \mathrm{diag}(\mathbf{w}) \cdot A^t$. □

4.3 Proof of the main theorem

In this section, we prove Theorem 4.7. To this end, the following Lemma is useful.

Lemma 4.25. *Let $(C_L(D, m_iQ))_{i=0,\dots,N}$ be a full flag of isometry-dual one-point AG codes with generator matrix A and let $(C_L(D', m'_jQ))_{j=0,\dots,n}$ be a full flag of induced punctured codes which is also isometry-dual with corresponding optimal generator matrix B with $wt(\mathbf{w}) = n$ is a vector as in Proposition 4.24. Then one pivot of $A\cdot\mathrm{diag}(\mathbf{w})\cdot A^t$ occurs at the very first column of the matrix. Moreover, any position of $A \cdot \mathrm{diag}(\mathbf{w}) \cdot A^t$ corresponding to the degree m, it is also a pivot.*

Proof. All components of the first column are of the form $\mathrm{ev}_D(f_1f_i)$ where each i is a geometric nongap. Let m to be the minimal i such that $\mathrm{ev}_D(f_1f_i) \neq 0$. There exists such m since f_1 is the constant function 1 and the matrix is of full rank. Then by definition, $(1, i)$ is a pivot position.

Suppose there exists functions f_i and f_j of A such that the degree of f_if_j is also m but $\mathrm{ev}_D(f_if_j) \cdot \mathbf{w} = 0$. Then f_if_j has pole order m at Q, so can be expressed as a linear combination of f_l with $l \leq m$. However $\mathrm{ev}_D(f_l) = 0$ for all $l < m$ and $\ell(mQ) - \ell((m-1)Q) = 1$, so this contradicts $\mathrm{ev}_D(f_1f_m) = \mathrm{ev}_D(f_m) \neq 0$. Therefore any components of the form $\mathrm{ev}_D(f_if_j) \cdot \mathbf{w}$ with $m_i + m_j = m$ is also a pivot. □

Now we give a proof of the main theorem.

proof of Theorem 4.7. Let A, B, m and $\mathbf{w}$ be as in the previous proof. By the previous Lemma, all positions with entry of the form $\mathrm{ev}_D(f_if_j) \cdot \mathbf{w}$ with $m_i + m_j = m$ are pivots. First, suppose that $m \geq 4g$ and see the following diagram.

				total of g gaps				
$-v_Q(f_i)$	0	1	$\cdots$	$2g-1$	$2g$	$2g+1$	$\cdots$	m
	$+$	$*$	$\cdots$	$*$	$+$	$+$	$\cdots$	$+$
	$+$	$+$	$\cdots$	$+$	$+$	$*$	$\cdots$	$+$
$-v_Q(f_j)$	m	$m-1$	$\cdots$	$m-2g+1$	$m-2g$	$m-2g-1$	$\cdots$	0
						total of g gaps		

where $*$ indicates that it is eitehr $+$ or $-$. In each column, the sum of the numbers at the very top and bottom are all m. If a number on the top row is a Weierstrass nongap(or gap), then the sign at the next row is $+$(or $-$ repectively). Similar for the bottom row and the third row. The shaded background indicates the cells that the sign is $+$. This is because all numbers greater than $2g-1$ are Weierstrass nongaps. Consider all pairs of functions f_i and f_j such that the pole order of f_if_j exactly m. We will show that the possible pivot positions are determined by the signs of columns.

1. For a column with $\begin{bmatrix} + \\ - \end{bmatrix}$ or $\begin{bmatrix} - \\ + \end{bmatrix}$ signs, the position corresponding to (f_i, f_j) is not a pivot.

   Since the $-$ sign indicates the Weierstrass gap number, there is no function having that exact pole number at Q. So, there is no such corresponding entries in the matrix.

2. Any colum with $\begin{bmatrix} + \\ + \end{bmatrix}$ signs corresponds to a pivot position.

   The signs imply that the correponding top and bottom numbers are Weierstrass nongap. So, there exist functions f_i and f_j with the corresponding pole order. Then $v_Q(f_if_j) = -m$. Note that this function is a linear combination of functions f_l with $l \leq m$. Write $f_if_j = \sum_{l\leq m} a_l f_l$. Then

   $$\begin{aligned}\big(\mathrm{ev}_D(f_i) * \mathbf{v}\big) \cdot \mathrm{ev}_D(f_j) &= \sum_{l<m} a_l \mathrm{ev}_D(f_l)\cdot\mathbf{v} + a_m \mathrm{ev}_D(f_m)\cdot\mathbf{v} \\ &= a_m \mathrm{ev}_D(f_m)\cdot\mathbf{v} \neq 0\end{aligned}$$

   since all f_l with $l < m$ are in the dual space of $f_1 = 1$ with respect to the dualizing vector $\mathbf{v}$, so that $\mathrm{ev}_D(f_l)\cdot\mathbf{v} = 0$. Therefore (f_i, f_j) corresponds to a pivot position.

3. There are no pivots other than these at positions corresponding to $[++]^t$.

   A pivot other than the $[++]^t$ case would correspond to a sign pattern

$-\ +$	$+\ -$
$+\ -$	$-\ +$

However, this cannot occur since pattern $[-+]^t$ and $[+-]^t$ are separated by the middle $[++]^t$ pattern at $(2g, 2g)$.

Since there are total of $m+1$ possible choices of pair of numbers adding to m and $2g$ of them are not pivots, there are exactly $m+1-2g$ pivots. Then $m = n+2g-1$. It follows that $n \geq 2g+1$. This proves (a).

Consider the case $m \leq 4g-2$. Also assume $m > 2g$ because if $m \leq 2g$ then it is obvious that $n \leq 2g$. If $m-2g$ is a nongap, then since $(2g, m-2g)$ corresponds to a pivot position, our previous argument works. So, let's assume that $m-2g$ is a gap. Let λ be the largest nongap which is smaller then $m-2g$. Consider the following alternative intervals:

Interval 1			Interval A			Interval 2		Interval A'		Interval 3		
0	$\cdots$	λ	$\lambda+1$	$\cdots$	$m-2g$	$\cdots$	$\cdots$	$2g$	$\cdots$	$m-\lambda$	$\cdots$	m
$+$	$\cdots$	$+$	$-$	$\cdots$	$-$	$\cdots$	$\cdots$	$+$	$\cdots$	$+$	$\cdots$	$+$
$+$	$\cdots$	$+$		$\cdots$	$+$	$\cdots$	$\cdots$	$-$	$\cdots$	$+$	$\cdots$	$+$
m	$\cdots$	$m-\lambda$		$\cdots$	$2g$	$\cdots$	$\cdots$	$m-2g$	$\cdots$	λ	$\cdots$	0

We count the number of columns in each interval by their type.

In Interval 1, there are total a of $\begin{bmatrix} - \\ + \end{bmatrix}$ and $\lambda+1-a$ of $\begin{bmatrix} + \\ + \end{bmatrix}$. In Interval 2, there are total b of $\begin{bmatrix} - \\ + \end{bmatrix}$, b number of $\begin{bmatrix} + \\ - \end{bmatrix}$ by symmetry, c of $\begin{bmatrix} - \\ - \end{bmatrix}$, and d of $\begin{bmatrix} + \\ + \end{bmatrix}$. In Interval A, there are total e of $\begin{bmatrix} - \\ + \end{bmatrix}$. In Interval A', total e of $\begin{bmatrix} + \\ - \end{bmatrix}$. In Interval 3, there are a $\begin{bmatrix} + \\ - \end{bmatrix}$ and $\lambda+1-a$ of $\begin{bmatrix} + \\ + \end{bmatrix}$.

Then we have the following by counting the Weierstrass gaps and the

length of Interval A and 2.

$$a + b + c + e = g \tag{4.1}$$
$$e = m - 2g - \lambda \tag{4.2}$$
$$2b + c + d = 2g - (m - 2g) - 1 = 4g - m - 1 \tag{4.3}$$

Note that each $\begin{bmatrix} + \\ + \end{bmatrix}$ column corresponds to a pivot position, called trivial pivots, and an ordered pair of $\begin{bmatrix} - \\ + \end{bmatrix}$ and $\begin{bmatrix} + \\ - \end{bmatrix}$ columns can possibly give a pivot. Then the number of pivots are bounded by the following:

$$\begin{aligned} n &\leq 2(\lambda + 1 - a) + d + b + e \\ &= 2\lambda + 2 - 2a + 4g - m - 1 - (b + c) + e && \text{by (4.3)} \\ &= 2\lambda + 4g - m + 1 - a + 2e - g && \text{by (4.1)} \\ &= 2\lambda + 3g - m + 1 - a + 2m - 4g - 2\lambda && \text{by (4.2)} \\ &= m + 1 - g - a && (4.4) \end{aligned}$$

Note that we get the following by the Clifford's theorem.

$$a \geq \frac{\lambda}{2} \tag{4.5}$$

since $\lambda + 1 - a = \ell(\lambda Q) \leq \dfrac{\lambda}{2} + 1$.

Counting Weierstrass gaps and nongaps in the interval $[0, 2g]$, we will get the following information.

$$\lambda + 1 - a + b + d + 1 = g + 1 \;\Rightarrow\; \lambda - a + b + d + 1 = g. \tag{4.6}$$
$$a + (m - 2g - \lambda) + b + c = g \qquad \text{from (4.1) + (4.2)}$$

We can combine them to get the following:

$$\begin{aligned} d - c &= 2a + m - 2g - 2\lambda - 1 \\ &\geq \lambda + m - 2g - 2\lambda - 1 && \text{applying (4.5)} \\ &= m - 2g - \lambda - 1 \geq 0 && \text{by the assumption } \lambda < m - 2g \end{aligned}$$

Hence, we get $d \geq c$.

Case1. $d = 0$. Then $c = 0$. Then number of gaps and nongaps are

$$\begin{array}{ll} \text{Nongaps(+)} & \lambda + 1 - a + b + 1 = g + 1 \quad \Rightarrow \quad \lambda - a + b + 1 = g. \\ \text{Gaps(-)} & a + (m - 2g - \lambda) + b = g. \end{array}$$

Then

$$\begin{array}{lll} \Rightarrow & \lambda + 1 - a + b = a + m - 2g - \lambda + b & \\ \Rightarrow & \lambda + 1 - a = a + m - 2g - \lambda & \\ \Rightarrow & 2\lambda + 1 = 2a + m - 2g \geq \lambda + m - 2g & \text{by (4.5)} \\ \Rightarrow & \lambda + 1 \geq m - 2g > \lambda & \end{array}$$

So,

$$\lambda + 1 = m - 2g \tag{4.7}$$

Then we get the following table

0	$\cdots$	λ	$m-2g$	$\cdots$	$\cdots$	$2g$	$m-\lambda$	$\cdots$	m
$+$	$\cdots$	$+$	$-$	$\cdots$	$\cdots$	$+$	$+$	$\cdots$	$+$
$+$	$\cdots$	$+$	$+$	$\cdots$	$\cdots$	$-$	$+$	$\cdots$	$+$
m	$\cdots$	$m-\lambda$	$2g$	$\cdots$	$\cdots$	$m-2g$	λ	$\cdots$	0

Then the number of pivots n is bounde by

$$\begin{aligned}
n &\leq m+1-g-a && \text{by (4.4)}\\
&= \lambda+1+g+1-a && \text{by (4.7)}\\
&= \lambda+g+2-a\\
&\leq \frac{\lambda}{2}+g+2 && \text{by (4.5)}\\
&= \frac{m-2g-1}{2}+g+2 && \text{by (4.7)}\\
&= \frac{m}{2}+\frac{3}{2}\\
&\leq 2g-1+\frac{3}{2}=2g+\frac{1}{2} && \text{by } m\leq 4g-2
\end{aligned}$$

Thus $n \leq 2g$.

Case2. d is nonzero.
Substitute g in (4.4) by (4.6),

$$n \leq m-\lambda-(b+d) \tag{4.8}$$

Subcase 1. If $b+d \geq e$. Then

$$\begin{aligned}
n &\leq m-\lambda-(b+d)\\
&\leq m-\lambda-e=2g && \text{since Interval A' has length } e
\end{aligned}$$

Then we are done.
Subcase 2. If $b+d<e$. Then

$$\begin{aligned}
g &= \lambda-a+b+d+1 && \text{by (4.6)}\\
&< \lambda-a+1+e\\
&= \lambda-a+1+m-2g-\lambda && \text{by (4.2)}\\
&= m-2g+1-a
\end{aligned}$$

Applying the above result to (4.1)+(4.2), we have

$$\begin{aligned} g = a + m - 2g - \lambda + b + c &< m - 2g - a + 1 \\ \Rightarrow 2a + b + c &< \lambda + 1 \\ \Rightarrow \lambda + b + c \leq 2a + b + c &< \lambda + 1 \qquad \text{by (4.5)} \\ \Rightarrow \lambda + b + c &< \lambda + 1 \\ \Rightarrow b + c &< 1 \end{aligned}$$

So, $b = c = 0$.

In this case, in Interval 2, there are only $\begin{bmatrix} + \\ + \end{bmatrix}$ columns, which completely separates Interval A and Interval A'. Then only trivial pivots occur and the number is bounded by

$$\begin{aligned} n &\leq 2(\lambda + 1 - a) + d \\ &\leq \lambda + 2 + d \qquad \text{by (4.5)} \\ &< \lambda + 2 + e \\ &= m - 2g + 2 \qquad \text{by (4.2)} \\ &\leq 4g - 2 - 2g + 2 = 2g \end{aligned}$$

This completes the proof of (b) in Theorem 4.7.

Lastly, assume that $m = 4g - 1$. Then the diagram is of the form

			total of g gaps			
$-v_Q(f_i)$	0	$\cdots$	$2g-1$	$2g$	$\cdots$	m
	$+$	$\cdots$	$*$	$+$	$\cdots$	$+$
	$+$	$\cdots$	$+$	$*$	$\cdots$	$+$
$-v_Q(f_j)$	m	$\cdots$	$2g$	$2g-1$	$\cdots$	0
				total of g gaps		

Then, in the middle, either of the following will happen.

Case 1	
$2g-1$	$2g$
$+$	$+$
$+$	$+$
$2g$	$2g-1$

Case 2	
$2g-1$	$2g$
$-$	$+$
$+$	$-$
$2g$	$2g-1$

Note that in Case 1, there are exactly $m+1-2g$ pivots correspond to the $[++]^t$ factors, so that $n = 2g$. Assume that Case 2 occurs. If $(2g, 2g)$ is not a pivot position then there are total of $m+1-2g = 2g$ pivots. If $(2g, 2g)$ is a pivot position then $n = 2g+1$. □

We conclude this section with examples that show the bound $n \geq 2g+2$ in Theorem is best possible.

Example 4.26. Let $\mathcal{X}$ be a Hermitian curve defined by an affine equation $y^2 + y = x^3$ over $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$ with $\alpha^2 + \alpha + 1 = 0$. Then the genus of $\mathcal{X}$ is 1.

Case 1. $m = 4g-1 = 3$ and $n = 2g+1$.

Let $D' = \{(0,1), (\alpha, \alpha), (\alpha^2, \alpha^2)\} \sim 2P_\infty + (0,0)$. Then we get the corresponding matrix

		0	2	3	4	5	6
1	0	0	0	1	1	1	1
x	2	0	1	1	1	1	0
y	3	1	1	0	1	1	0
x^2	4	1	1	1	0	0	1
xy	5	1	1	1	0	0	1
x^3	6	1	0	0	1	1	1

with a dualizing vector $v = (1, a^2, a)$.

$$I(D') = (F = y^2 + y - x^3, f_4 = x^2 + y + 1, f_5 = xy + y + 1).$$

Case 2. $m = 4g = 4$ and $n = 2g+1$.

From $m = 4g$, it has to be that $n = m - 2g + 1$.

		0	2	3	4	5	6
1	0	0	0	0	1	1	1
x	2	0	1	1	1	1	0
y	3	0	1	1	1	1	0
x^2	4	1	1	1	0	0	1
xy	5	1	1	1	0	0	1
x^3	6	1	0	0	1	1	1

with a dualizing vector $v = (1, a^2, a)$.

$$I(D') = (F = y^2 + y - x^3, f_3 = y + x).$$

Also, consider the Hermitian curve $\mathcal{X}$ given by the equation $y^3 + y = x^4$ over $\mathbb{F}_9 = \mathbb{F}_3[\alpha]$ with $\alpha^2 - \alpha - 1 = 0$. This has genus 3.

Case 1. $m = 4g - 1 = 11$.

Choose D' be such that

$$\begin{aligned} D' &= \{(0, a^2), (0, a^6), (1, 2), (a, 1), (a^3, 1), (a^5, a^7), (a^7, a^5)\} \\ &\sim 6P_\infty + (0, 0). \end{aligned}$$

Then we will get the matrix

		0	3	4	6	7	8	9	10	11	12
1	0	0	0	0	0	0	0	0	0	1	1
x	3	0	0	0	0	0	1	1	1	0	2
y	4	0	0	0	0	1	1	1	0	2	1
x^2	6	0	0	0	1	1	0	2	1	1	2
xy	7	0	0	1	1	0	2	1	1	2	1
y^2	8	0	1	1	0	2	1	1	2	0	0
x^3	9	0	1	1	2	1	1	2	1	0	2
x^2y	10	0	1	0	1	1	2	1	0	1	1
xy^2	11	1	0	2	1	2	0	0	1	1	1
x^4	12	1	2	1	2	1	0	2	1	1	1

with a dualizing vector $v = (1, 1, 2, a^7, a^5, a, a^3)$.

$$I(D') = (F = y^3+y-x^4, f_9 = x^3+x^2-y^2-1, f_{10} = x^2y+x^2+xy-y^2-1).$$

Case 2. $m = 4g = 12$.

Note that it has to be that $n = 2g + 1 = 7$. Let

$$\begin{aligned} D' &= \{(1, a), (1, a^3), (1, 2), (a, 1), (a^3, 1), (a^5, 1), (a^7, 1)\} \\ &\sim 7P_\infty. \end{aligned}$$

Then the matrix is

		0	3	4	6	7	8	9	10	11	12
1	0	0	0	0	0	0	0	0	0	0	1
x	3	0	0	0	0	0	0	1	0	0	1
y	4	0	0	0	0	0	1	0	0	1	1
x^2	6	0	0	0	1	0	0	1	1	0	1
xy	7	0	0	0	0	0	1	1	0	1	1
y^2	8	0	0	1	0	1	1	0	1	1	1
x^3	9	0	1	0	1	1	0	1	1	1	1
x^2y	10	0	0	0	1	0	1	1	1	1	1
xy^2	11	0	0	1	0	1	1	1	1	1	1
x^4	12	1	1	1	1	1	1	1	1	1	0

with a dualizing vector $v = (a^5, a^7, 2, a^2, a^6, a^7, a^5)$.

$$I(D') = (F = y^3 + y - x^4, f_7 = xy - y - x + 1).$$

4.4 Examples

In this section we suggest various examples of isometry-dual codes and its preservation by puncturing. We first suggest two cases of one-point AG codes, one on the Hermitian curve and the other on Klein curve. Then we give an example of Reed-Muller type code, which is not defined on any specific curve

but given on affine plane.

4.4.1 Hermitian curve

The Hermitian curve $\mathcal{X}$ over $\mathbb{F}_{q^2}$ for some prime p power q is given by the affine equation $x^{q+1} = y^q + y$. It is a smooth curve of genus $g = q(q-1)/2$. There are a total of $q^3 + 1$ rational points on the curve, one of which is at infinity. Let $q = 2$ and α be the class of T in $\mathbb{F}_4 = \mathbb{F}_2[T]/(T^2 + T + 1)$. Denote the eight affine rational points by

$$\begin{array}{lllll} l_1\text{:} & P_1 = (0,0), & P_2 = (0,1), & & \\ l_2\text{:} & P_3 = (1,\alpha), & P_4 = (\alpha,\alpha), & P_5 = (\overline{\alpha},\alpha), & \\ l_3\text{:} & P_6 = (1,\overline{\alpha}), & P_7 = (\alpha,\overline{\alpha}), & P_8 = (\overline{\alpha},\overline{\alpha}) & \end{array}$$

where l_i for $i = 1, 2, 3$ is a line passing through the points on the same row. Let $D = P_1 + \ldots + P_8$. The canonical divisor K is equivalent to 0. The following table gives data of i and m_i for the flag $(C_L(D, m_iQ))_{i=0,\ldots,8}$ being isometry dual.

i	0	1	2	3	4	5	6	7	8
m_i	-1	0	2	3	4	5	6	7	9

Then a generator matrix of the code $C_L(D, m_8Q)$ is given by

	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8
1	1	1	1	1	1	1	1	1
x	0	0	1	α	$\overline{\alpha}$	1	α	$\overline{\alpha}$
y	0	1	α	α	α	$\overline{\alpha}$	$\overline{\alpha}$	$\overline{\alpha}$
x^2	0	0	1	$\overline{\alpha}$	α	1	$\overline{\alpha}$	α
xy	0	0	α	$\overline{\alpha}$	1	$\overline{\alpha}$	1	α
x^3	0	0	1	1	1	1	1	1
x^2y	0	0	α	1	$\overline{\alpha}$	$\overline{\alpha}$	α	1
x^3y	0	0	α	α	α	$\overline{\alpha}$	$\overline{\alpha}$	$\overline{\alpha}$

where the very left column denotes functions in $L(m_iQ) \backslash L((m_i - 1)Q$ on which the points of D are evaluated. That the flag $(C_L(D, m_iQ))_{i=0,\ldots,8}$ is

isometry-dual can be obtained from the fact

$$K + D \sim D \sim 8Q.$$

and applying Theorem 4.2. The dualizing vector is $\mathbf{v} = (1, 1, \ldots, 1)$. Note that on an elliptic curve, an intersection of a line with the curve corresponds to the identity according to the group law and we get the following.

$$\begin{aligned} 3Q &\sim P_3 + P_4 + P_5 \\ &\sim P_6 + P_7 + P_8 \end{aligned}$$

Thus if $D_5 := P_1 + \ldots + P_5$, the punctured codes $(C_L(D_5, m'_j Q))_{j=0,\ldots,5}$ is also isometry-dual with the following generator matrix.

pole order at Q	function	P_1	P_2	P_3	P_4	P_5
0	1	1	1	1	1	1
2	x	0	0	1	α	$\overline{\alpha}$
3	y	0	1	α	α	α
4	x^2	0	0	1	$\overline{\alpha}$	α
6	x^3	0	0	1	1	1

with a dualizing vector $(1, \overline{\alpha}, \alpha, \alpha, \alpha)$. This agrees with the Theorem 4.6 that $|D| - |D_5| = 3$ is a Weierstrass nongap.

Further, if we set $D_2 = P_1 + P_2$, the induced code is also isometry-dual, which is obvious from the following matrix

pole order at Q	function	P_1	P_2
0	1	1	1
3	y	0	1

with a dualizing vector $(1, 1)$. Note that $|D_2| \not\geq 2g + 2$, so not in the range of the condition of Theorem 4.2.

4.4.2 Klein curve

The Klein curve $\mathcal{X}$ is given by $X^3Y + Y^3Z + Z^3X = 0$ in a projective plane over a field of characteristic 2. There are three $\mathbb{F}_2$-rational poins of $\mathcal{X}$, namely,

$Q_1 = (1:0:0)$, $Q_2 = (0:1:0)$, and $Q_3 = (0:0:1)$. Let $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$ such that $\alpha^3 + \alpha + 1 = 0$. Note that $\alpha^7 = 1$. The $\mathbb{F}_8$-rational points on $\mathcal{X}$, which are not Q_i for $i = 1, 2, 3$ are given as follows:

$$\begin{array}{lllll}
l_1: & P_1 = (1:\alpha:1), & P_2 = (1:\alpha^2:1), & P_3 = (1:\alpha^4:1), \\
l_2: & P_4 = (1:1:\alpha), & P_5 = (1:\alpha^4:\alpha), & P_6 = (1:\alpha^5:\alpha), \\
l_3: & P_7 = (1:1:\alpha^2), & P_8 = (1:\alpha:\alpha^2), & P_9 = (1:\alpha^3:\alpha^2), \\
l_4: & P_{10} = (1:\alpha^3:\alpha^3), & P_{11} = (1:\alpha^4:\alpha^3), & P_{12} = (1:\alpha^6:\alpha^3), \\
l_5: & P_{13} = (1:1:\alpha^4), & P_{14} = (1:\alpha^2:\alpha^4), & P_{15} = (1:\alpha^6:\alpha^4), \\
l_6: & P_{16} = (1:\alpha^2:\alpha^5), & P_{17} = (1:\alpha^3:\alpha^5), & P_{18} = (1:\alpha^5:\alpha^5), \\
l_7: & P_{19} = (1:\alpha:\alpha^6), & P_{20} = (1:\alpha^5:\alpha^6), & P_{21} = (1:\alpha^6:\alpha^6)
\end{array}$$

where points on each row are colinear on the line l_i for $i = 1, \ldots, 7$. Recall some properties of the Klein curve.

1. The genus of $\mathcal{X}$ is 3.

2. There are a total of twenty four $\mathbb{F}_8$-rational points, all of which are flexpoints.

3. A tangent line to any of the twenty four points meets three times with the curve $\mathcal{X}$ at the point and at other $\mathbb{F}_8$-rational point. Denote T_Q the tangent line of the curve $\mathcal{X}$ at Q, i.e. $I(Q, T_Q \cap \mathcal{X}) = 3$ for all rational points Q of $\mathcal{X}$.

4. For any F_8-rational point Q of $\mathcal{X}$, there exists two distinct points, written as Q' and Q'', such that

$$\begin{aligned}
I(Q', T_Q \cap \mathcal{X}) &= 1 \\
I(Q'', T_{Q'} \cap \mathcal{X}) &= 1 \\
I(Q, T_{Q''} \cap \mathcal{X}) &= 1
\end{aligned}$$

5. With the previous notation of Q, Q', Q'', the canonical divisor L satisfies

$$L \sim 3Q + Q' \sim 3Q' + Q'' \sim 3Q'' + Q$$

6. Consider any two F_8-rational points R_1 and R_2 none of each is on the tangent line of the other. Then the line through R_1 and R_2 meets $\mathcal{X}$ at four distinct points. We write these two points by R_3 and R_4.

7. With the previous notation for R_1, R_2, R_3, and R_4, the canonical divisor L satisfies
$$L \sim R_1 + R_2 + R_3 + R_4$$

8. Allowing redundancies, there are a total of ${}_{24}C_2 = 276$ lines passing through two distinct $\mathbb{F}_8$-rational points of $\mathcal{X}$. Twenty four of them are tangent lines at each points. The remaining 252 are 42 passing througth 4 distinct points of $\mathcal{X}$. So, we get the computation $24 + 6 \times 42 = 276$.

9. The Weierstrass nongaps at a point Q are given the following.

m	0	1	2	3	4	5	6	7	8	9	$\cdots$
mQ	+	−	−	+	−	+	+	+	+	+	$\cdots$

   Note that the Weierstrass semigroup of nongaps at Q is generated by 3, 5, and 7.

Let $Q = Q_3 = (0 : 0 : 1)$. Choose the following three functions:

$u := Z/X$	pole order 3 at Q
$v := YZ/X^2$	pole order 5 at Q
$w := Y^2Z/X^3$	pole order 7 at Q

Here, we suggest divisors D_n given by a sum of n $\mathbb{F}_8$-rational points such that the one-point AG codes $C_L(D, mQ)$ satisfies the isometry-dual property. Let $Q = Q_3 = (0 : 0 : 1)$ and consider a one-point AG code at Q. Define $D_2 = Q' + Q''$, where $Q' = (0 : 1 : 0)$ and $Q'' = (1 : 0 : 0)$. Note that

$$\begin{aligned} K + D_2 &\sim 3Q + Q' + Q' + Q'' = 3Q + (3Q' + Q'') - Q' \\ &\sim 3Q + K - Q' \\ &\sim 6Q \end{aligned}$$

The gap structure with $mQ - D_2$ is given by

m	0	1	2	3	4	5	6	7	8	9	$\cdots$
mQ	+	−	−	+	−	+	+	+	+	+	$\cdots$
$mQ - D_2$	−	−	−	+	−	+	+	−	+	+	

Note that

$$1 \in L(0Q) \backslash L(0Q - D_2)$$
$$w \in L(7Q) \backslash L(7Q - D_2)$$

and we get the 2×2 generating matrix

	Q'	Q''
1	1	1
w	1	0

Let $D_5 = Q' + Q'' + P_1 + P_2 + P_3$, where P_1, P_2, P_3, and Q' are collinear. Then

$$K + D_5 \sim 6Q + P_1 + P_2 + P_3 + Q' - Q'$$
$$\sim 6Q + K - Q' \sim 9Q$$

and $D_5 - D_2 \sim 3Q$.

The gap structure with $mQ - D_5$ is given by

	0	1	2	3	4	5	6	7	8	9	10	11	$\cdots$
mQ	+	−	−	+	−	+	+	+	+	+	+	+	$\cdots$
$mQ - D_5$	−	−	−	−	−	−	+	−	+	+	−	+	$\cdots$

Note that

$$u \in L(3Q) \backslash L(3Q - D_5)$$
$$v \in L(5Q) \backslash L(5Q - D_5)$$
$$v^2 \in L(10Q) \backslash L(10Q - D_5)$$

and we get the 5×5 generating matrix

	Q'	Q''	P_1	P_2	P_3
1	1	1	1	1	1
u	0	0	1	1	1
v	0	0	w	w^2	w^4
w	1	0	w^2	w^4	w
v^2	0	0	w^2	w^4	w

with the dualizing vector of the above matrix is $(1, 1, w, w^2, w^4)$. Note that the yellow background indicates how the 2×2 generating matrix for D_2 case embeds.

Let $D_8 = D_5 + P_4 + P_5 + P_6$. Then

$$\begin{aligned} K + D_8 &= K + D_5 + P_4 + P_5 + P_6 \\ &\sim 9Q + K - Q' \\ &\sim 12Q \end{aligned}$$

with $D_8 - D_5 \sim 3Q$ and $D_8 - D_2 \sim 6Q$.

The gap structure with $mQ - D_8$ is given by

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	$\cdots$
mQ	+	−	−	+	−	+	+	+	+	+	+	+	+	+	+	$\cdots$
$mQ - D_5$	−	−	−	−	−	−	−	−	−	+	−	+	+	−	+	$\cdots$

Note that

$$\begin{aligned} u^2 &\in L(6Q) \backslash L(6Q - D_8) \\ uv &\in L(8Q) \backslash L(8Q - D_8) \\ uv^2 &\in L(13Q) \backslash L(13Q - D_8) \end{aligned}$$

and we get the 8×8 generating matrix

	Q'	Q''	P_1	P_2	P_3	P_4	P_5	P_6
1	1	1	1	1	1	1	1	1
u	0	0	1	1	1	w	w	w
v	0	0	w	w^2	w^4	w	w^5	w^6
u^2	0	0	1	1	1	w^2	w^2	w^2
w	1	0	w^2	w^4	w	w	w^2	w^4
uv	0	0	w	w^2	w^4	w^2	w^6	1
v^2	0	0	w^2	w^4	w	w^2	w^3	w^5
uv^2	0	0	w^2	w^4	w	w^3	w^4	w^6

with the dualizing vector $(w^6, w^6, w^5, w^6, w, 1, w^4, w^5)$. The shadowed background indicates the embedding of 5×5 matrix for the D_5.

Lemma 4.27. *Let $n = 3i + 2$ and $D_n = Q' + Q'' + P_1 + \cdots + P_{3i}$. Then*

$$K + D_n \sim (n + 2g - 2)Q$$

for $i = 0, \ldots, 7$.

Proof. It was proven for the case $i = 0, 1, 2$ in the above. From the construction of P_i for $i = 1, \ldots, 21$, we know that Q', P_{3i+1}, P_{3i+2}, and P_{3i+3} are colinear for $i = 0, \ldots, 6$. Then

$$\begin{aligned} K + D_{n+3} &= K + D_n + P_{3i+1} + P_{3i+2} + P_{3i+3} \\ &\sim (n + 2g - 2)Q + L - Q' \\ &\sim (n + 3 + 2g - 2)Q \end{aligned}$$

where L denotes the canonical divisor $Q' + P_{3i+1} + P_{3i+2} + P_{3i+3}$. □

Hence finding set of points which are colinear on a line passing Q' will give a set of divisors satisfying isometry-dual condition on the corresponding one-point AG codes. For D_{23} we have the following gap structure:

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
mQ	+	−	−	+	−	+	+	+	+	+	+	+	+	+	+	+
$mQ - D_{23}$	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−

	16	17	18	19	20	21	22	23	24	25	26	27	28	29	$\cdots$
mQ	+	+	+	+	+	+	+	+	+	+	+	+	+	+	$\cdots$
$mQ - D_{23}$	−	−	−	−	−	−	−	−	+	−	+	+	−	+	$\cdots$

Let's consider the following functions f_i whose pole order at Q is i

	1	u	u^2	u^3	u^4
1	$f_0 = 1$	$f_3 = u$	$f_6 = u^2$	$f_9 = u^3$	$f_{12} = u^4$
v	$f_5 = v$	$f_8 = uv$	$f_{11} = u^2v$	$f_{14} = u^3v$	$f_{17} = u^4v$
v^2	$f_{10} = v^2$	$f_{13} = uv^2$	$f_{16} = u^2v^2$	$f_{19} = u^3v^2$	$f_{22} = u^4v^2$
v^3	$f_{15} = v^3$	$f_{18} = uv^3$	$f_{21} = u^2v^3$		
v^4	$f_{20} = v^4$	$f_{23} = uv^4$			
v^5	$f_{25} = v^5$	$f_{28} = uv^5$			

and $f_7 = w$.

4.4.3 Reed Muller type code

Consider the affine space $\mathbb{F}_2^m$. It is m dimensional vector space over $\mathbb{F}_2$, so elements are of the form $(\alpha_m, \alpha_{m-1}, \ldots, \alpha_1)$ where each $\alpha_j \in \mathbb{F}_2 = \{0, 1\}$ for $j = 1, \ldots, m$. Let x_{α_j} be the coordinate functions for $j = 1, \ldots, m$, that is, $x_{\alpha_j}(\alpha_m, \alpha_{m-1}, \ldots, \alpha_1) = \alpha_j$ for $j = 1, \ldots, m$. Note that $x_{\alpha_j}^2 = x_{\alpha_j}$. Then the coordinate ring is $R = \mathbb{F}_2[x_1, x_2, \ldots, x_m]/I$ for $I = (x_1^2 - x_1, x_2^2 - x_2, \ldots, x_m^2 - x_m)$, which is, as a set, a set of square free monomials in $x_1, \ldots, x_m$. Let $\alpha = (\alpha_m, \alpha_{m-1}, \ldots, \alpha_1)$ and $\beta = (\beta_m, \beta_{m-1}, \ldots, \beta_1)$ be vectors in $\mathbb{F}_2^m$. We write x^α for the function $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_m^{\alpha_m}$. An order on R is defined by $x^\alpha < x^\beta$ if and only if

1. Either $\sum \alpha_i < \sum \beta_i$
2. or $\sum \alpha_i = \sum \beta_i$ and $\exists j$ such that $\alpha_j = 0$, $\beta_j = 1$ and $\alpha_k = \beta_k$ for all

$k = j + 1, \ldots, m.$

Call this by `DegLex` order. There is a bijection between $\mathbb{F}_2$-rational points of $\mathbb{F}_2^m$ and functions in the coordinate ring R by $\alpha \longleftrightarrow x^\alpha$. We copy the `DegLex` order on R to $\mathbb{F}_2^m$. For a function $f = X^\alpha$ and a point $P = \beta$,

$$f(P) = \begin{cases} 1 & \text{if } x^\alpha | x^\beta \\ 0 & \text{otherwise} \end{cases}$$

Let $N = 2^m$. Define an $N \times N$ matrix $A = (A_{f,P})$ with rows of functions in R and columns of affine points in $\mathbb{F}_2^m$ both indexed by `DegLex` order. Then with this orders on points and functions, we get an isometry-dual matrix. For $m = 3$, we get the following matrix A.

	000	001	010	100	011	101	110	111
1	1	1	1	1	1	1	1	1
x_1	0	1	0	0	1	1	0	1
x_2	0	0	1	0	1	0	1	1
x_3	0	0	0	1	0	1	1	1
x_1x_2	0	0	0	0	1	0	0	1
x_1x_3	0	0	0	0	0	1	0	1
x_2x_3	0	0	0	0	0	0	1	1
$x_1x_2x_3$	0	0	0	0	0	0	0	1

Then it can be easily checked that this matrix is isometry-dual with the dualizing vector $(1, 1, \ldots, 1)$, that is, we get

$$AA^T = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

For a subset of n rational points, the corresponding columns in A define

a $N \times n$ submatrix whose row spaces define a flag of length n from 0 to $\mathbb{F}_2^n$. From this $N \times n$ matrix choose n rows in a way that the chosen row is linearly independent on the previous rows. Then we get a full flag of $\mathbb{F}_2^n$ generated by first i rows of the $n \times n$ matrix. We are interested in the case when this choice gives an isometry-dual flag. The next two tables give the relevant minors that define the flag for the subsets of points $\{000, 001, 010, 011\}$ and $\{000, 001, 010, 111\}$.

	000	001	010	011
1	1	1	1	1
x_1	0	1	0	1
x_2	0	0	1	1
x_1x_2	0	0	0	1

	000	001	010	111
1	1	1	1	1
x_1	0	1	0	1
x_2	0	0	1	1
x_3	0	0	0	1

The two subsets share the same minors and thus the same flags. Both are isometry-dual. For the first subset this follows immediately with the observation that the set is the set of all rational points in affine space of dimension 2, that is, it is in the affine plane which is a hyperplane of a coordinate function x_3. The vanishing ideals for the two sets of points are

$$I(\{000, 001, 010, 011\}) = (x_3),$$
$$I(\{000, 001, 010, 111\}) = (x_1x_2 + x_3, x_1x_3 + x_3, x_2x_3 + x_3).$$

There are a total of 22 isometry-dual subsets of size 4. The row span R_5 of the first five rows in the 8-by-8 matrix A, the rows labeled $1, x_1, x_2, x_3x_1x_2$, contains 32 vectors, with weight distribution $0\,(1\times), 2\,(4\times), 4\,(22\times), 6\,(4\times), 8\,(1\times)$. The 22 vectors of weight 4 are the characteristic vectors of the 22 isometry-dual subsets of size 4. They divide into four groups: 2 are in $R_2\backslash R_1$, 4 are in $R_3\backslash R_2$, 8 are in $R_4\backslash R_3$, and 8 are in $R_5\backslash R_4$. Minors for subsets in the same group share the same rows.

$$R_2\backslash R_1 : 1, x_2, x_3, x_2x_3 \ (2\times)$$
$$R_3\backslash R_2 : 1, x_1, x_3, x_1x_3 \ (4\times)$$
$$R_4\backslash R_3 : 1, x_1, x_2, x_1x_2 \ (8\times)$$
$$R_5\backslash R_4 : 1, x_1, x_2, x_3 \ (8\times)$$

Let $v = (1,1,1,0,0,0,0,1)$ be the characteristic vector for the subset $\{000, 001, 010, 111\}$.

$$A\text{diag}(v)A^T = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Proposition 4.28. *There are* $54 = 2^6 - 10$ *isometry-dual subsets of size 8 in affine space* F^4*. Their characteristic vectors are the vectors of weight 8 in the row span* R_6 *of rows* $1, x_1, x_2, x_3, x_4, x_1x_2$ *in* A*. The weight distribution of the row span is* $0^1 4^4 8^{54} 12^4 16^1$*. The 54 subsets divide into 6 orbits of sizes* $2, 4, 8, 16, 8, 16$*. Pivots in positions* $(x^\alpha, x^{\alpha'})$*:*

$$x^\alpha x^{\alpha'} = \begin{cases} x_2x_3x_4 & (2\times) \\ x_1x_3x_4 & (4\times) \\ x_1x_2x_4 & (8\times) \\ x_1x_2x_3 & (16\times) \\ x_3x_4 \text{ or } x_1x_2x_4 & (8\times) \\ x_3x_4 \text{ or } x_1x_2x_3 & (16\times) \end{cases}$$

Ideals that represent the different groups

$$I = \begin{cases} (x_1) \\ (x_2) \\ (x_3) \\ (x_4) \\ (x_3 + x_1x_2,\ x_3 + x_1x_3,\ x_3 + x_2x_3) \\ (x_4 + x_1x_2,\ x_4 + x_1x_4,\ x_4 + x_2x_4) \end{cases}$$

Proposition 4.29. *There are* $118 = 2^7 - 10$ *isometry-dual subsets of size 16 in affine space* F^5*. Their characteristic vectors are the vectors of weight*

16 in the row span R_7 of rows $1, x_1, x_2, x_3, x_4, x_5, x_1x_2$ in A. The weight distribution of the row span is $0^1 8^4 16^{118} 24^4 32^1$. The 118 subsets divide into 8 orbits of sizes $2, 4, 8, 16, 32, 8, 16, 32$.

Bibliography

[1] Valentina Barucci, *Decompositions of ideals into irreducible ideals in numerical semigroups*, Journal of Commutative Algebra **2** (2010), no. 3, 281–294.

[2] M. Bras Amorós, *A Note on the Inheritance of the Isometry-Dual Property under Puncturing AG Codes*, ArXiv e-prints (2017).

[3] Maria Bras-Amorós, Kwankyu Lee, and Albert Vico-Oton, *New lower bounds on the generalized hamming weights of AG codes.*, IEEE Trans. Information Theory **60** (2014), no. 10, 5930–5937.

[4] Xing Chao-Ping, *When are two geometric goppa codes equal?*, IEEE transactions on information theory **38** (1992), no. 3, 1140–1142.

[5] Arnaldo García and Henning Stichtenoth, *Elementary abelian p-extensions of algebraic function fields*, manuscripta mathematica **72** (1991), no. 1, 67–79.

[6] Olav Geil, Carlos Munuera, Diego Ruano, and Fernando Torres, *On the order bounds for one-point AG codes*, Advances in Mathematics of Communications **5** (2011), no. 3, 489–504.

[7] Valerii Denisovich Goppa, *Codes on algebraic curves*, Soviet Math. Dokl. **24** (1981), no. 1, 170–172.

[8] David Goss, *Basic structures of function field arithmetic*, Springer-Verlag, 1998.

[9] James William Peter Hirschfeld, Gábor Korchmáros, and Fernando Torres, *Algebraic curves over a finite field*, vol. 43, Princeton University Press, 2013.

[10] Carlos Munuera and Ruud Pellikaan, *Equality of geometric Goppa codes and equivalence of divisors*, Journal of Pure and Applied Algebra **90** (1993), no. 3, 229–252.

[11] Oystein Ore, *On a special class of polynomials*, Transactions of the American Mathematical Society **35** (1933), no. 3, 559–584.

[12] Henning Stichtenoth, *Algebraic function fields and codes*, vol. 254, Springer, 2009.